(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号
特開2001－117820
（P2001－117820A）
(43)公開日　平成13年４月27日(2001.4.27)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｚ　５Ｂ０１７

審査請求　未請求　請求項の数15　ＯＬ　（全 29 頁）

(21)出願番号　特願平11－293544

(22)出願日　平成11年10月15日(1999.10.15)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　黒田　康嗣
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72)発明者　吉岡　孝司
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

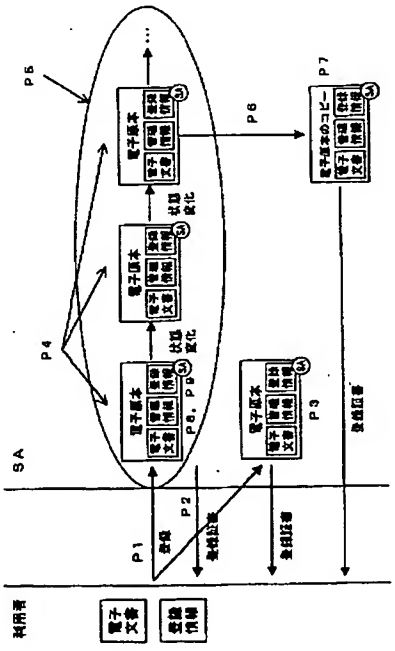
(74)代理人　100074099
弁理士　大菅　義之　（外１名）

最終頁に続く

(54)【発明の名称】　電子原本管理装置および方法

(57)【要約】
【課題】　電子化された重要文書の原本をより安全に管理することが課題である。
【解決手段】　利用者のコンピュータ環境とは別に電子原本管理装置を設けて、電子文書を電子原本として登録する。電子原本管理装置は、電子原本を一意に識別するための登録証書を発行し、利用者は、発行された登録証書を用いて電子原本にアクセスする。

電子原本モデルを示す図



1

【特許請求の範囲】
【請求項１】　電子情報を原本情報として登録する登録手段と、
前記電子情報に対して、該電子情報を論理的に一意に識別する論理識別情報と、該電子情報の物理的所在を表す所在識別情報とを付与する付与手段と、
前記論理識別情報と前記所在識別情報の組合せに基づく組合せ識別情報を用いて、前記原本情報を管理する管理手段と、
前記組合せ識別情報を含み、前記原本情報へのアクセスのために用いられる登録証書情報を発行する発行手段とを備えることを特徴とする電子原本管理装置。
【請求項２】　利用者は、前記登録証書情報に含まれる前記組合せ識別情報を用いて、前記電子原本管理装置に登録された前記原本情報にアクセスすることを特徴とする請求項１記載の電子原本管理装置。
【請求項３】　前記管理手段は、前記所在識別情報と前記電子情報が保存されている物理的所在とを比較し、該所在識別情報が該物理的所在に対応していなければ、該電子情報は不正コピーであると判断することを特徴とする請求項１記載の電子原本管理装置。
【請求項４】　前記電子原本管理装置の識別情報、装置内の電子情報識別情報、オリジナルとコピーを識別するためのタイプ属性情報、およびタイムスタンプ情報から前記論理識別情報を作成する作成手段をさらに備え、前記管理手段は、該電子原本管理装置の識別情報と電子情報識別情報の組合せを原本系列識別情報として管理することを特徴とする請求項１記載の電子原本管理装置。
【請求項５】　前記管理手段は、登録される電子情報をすべて原本情報として扱い、登録時には、オリジナルを表すタイプ属性情報を該登録される電子情報に付与することを特徴とする請求項４記載の電子原本管理装置。
【請求項６】　前記電子情報のコピーの作成時には、前記管理手段は、前記原本系列識別情報と前記タイムスタンプ情報を変更せず、前記タイプ属性情報をコピーを表すタイプ属性情報に変更した論理識別情報を生成し、生成された論理識別情報を該電子情報のコピーに付与することを特徴とする請求項５記載の電子原本管理装置。
【請求項７】　利用者は、前記登録証書情報に含まれる前記タイプ属性情報を参照することで、前記電子情報がオリジナルであるかコピーであるかを判断することを特徴とする請求項４記載の電子原本管理装置。
【請求項８】　前記電子情報がコピーであるとき、前記利用者は、前記登録証書情報に含まれる前記タイムスタンプ情報を参照することで、該コピーがどの時点の電子情報のコピーであるかを判断することを特徴とする請求項７記載の電子原本管理装置。
【請求項９】　前記原本情報の更新時には、前記管理手段は、前記原本系列識別情報と前記タイプ属性情報を変更せず、前記タイムスタンプ情報を変更して、更新前と

2

更新後の原本情報を管理することを特徴とする請求項４記載の電子原本管理装置。
【請求項１０】　前記管理手段は、前記原本情報の時系列な変化に応じて原本情報の一連のインスタンスを生成し、該一連のインスタンスを１つの原本系列として扱うことを特徴とする請求項４記載の電子原本管理装置。
【請求項１１】　前記電子原本管理装置に他の電子原本管理装置から原本情報が移動してきたとき、前記管理手段は、移動してきた原本情報の原本系列識別情報とタイプ属性情報を変更せず、タイムスタンプ情報を変更して、該移動してきた原本情報を管理することを特徴とする請求項４記載の電子原本管理装置。
【請求項１２】　電子情報の時系列な変化に応じて、対応する原本情報の一連のインスタンスを生成し、該一連のインスタンスを１つの原本系列として管理する管理手段と、
前記原本系列に対して原本系列識別情報を付与する付与手段と、
前記原本系列識別情報を含み、前記一連のインスタンスのうちの１つのインスタンスへのアクセスのために用いられる登録証書情報を発行する発行手段とを備えることを特徴とする電子原本管理装置。
【請求項１３】　電子情報を論理的に一意に識別する論理識別情報と該電子情報の物理的所在を表す所在識別情報との組合せに基づく組合せ識別情報を含む登録証書情報を格納する格納手段と、
前記登録証書情報を用いて、原本情報として登録された前記電子情報へのアクセスを要求する要求手段とを備えることを特徴とする電子原本アクセス装置。
【請求項１４】　電子情報を原本情報として登録し、
前記電子情報に対して、該電子情報を論理的に一意に識別する論理識別情報と、該電子情報の物理的所在を表す所在識別情報とを付与し、
前記論理識別情報と前記所在識別情報の組合せに基づく組合せ識別情報を用いて、前記原本情報を管理し、
前記組合せ識別情報を含む登録証書情報を用いて、前記原本情報にアクセスすることを特徴とする電子原本管理方法。
【請求項１５】　電子情報の時系列な変化に応じて、対応する原本情報の一連のインスタンスを生成し、
前記一連のインスタンスを１つの原本系列として管理し、
前記原本系列に対して原本系列識別情報を付与し、
前記原本系列識別情報を含む登録証書情報を用いて、前記一連のインスタンスのうちの１つのインスタンスにアクセスすることを特徴とする電子原本管理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、文書の電子化に係り、電子化された重要文書の原本を管理する装置および

方法に関する。

【０００２】

【従来の技術】従来、重要文書の原本は紙媒体として管理され、それらは、ファイリングして整理したりして管理されてきた。しかし、近年のパーソナルコンピュータの普及とネットワーク環境の拡大により、企業間取引や電子決済等の様々なサービスの電子化が進展し、紙媒体として扱われてきた重要文書が電子媒体に記録されて処理されている。電子化が進むにつれて、データベースと連携した文書管理アプリケーションが出現し、現在、それらのアプリケーションを用いて文書が管理されつつある。

【０００３】

【発明が解決しようとする課題】しかしながら、従来の文書管理アプリケーションには、以下のような問題がある。

１．利用者の管理下のコンピュータで文書が管理されるため、文書の作成日時等を容易に偽れる。

２．利用者の管理下のコンピュータで文書が管理されるため、文書を容易に削除可能である。

３．利用者の管理下のコンピュータで文書が管理されるため、文書を容易に改ざん可能である。たとえ、文書管理アプリケーションが文書操作の履歴を記録していたとしても、その履歴をも容易に改ざんすることができる。

４．文書をコピーすると、全く同じ内容の電子文書ができてしまうため、どちらが本物の原本であるかわからなくなる。

【０００４】このように、電子化文書には紙媒体にない様々な問題があるため、重要文書の電子化においては、運用面での制限が紙媒体以上に課せられている。このため、せっかく電子処理されるにもかかわらず、最終的には文書を紙媒体に出力して、契約や発注の処理を行ったり、法廷文書として保管しているのが現状である。

【０００５】本発明の課題は、電子化された重要文書の原本をより安全に管理する装置および方法を提供することである。

【０００６】

【課題を解決するための手段】図１は、本発明の電子原本管理装置の原理図である。図１の電子原本管理装置は、登録手段１、付与手段２、管理手段３、および発行手段４を備える。

【０００７】本発明の第１の局面において、登録手段１は、電子情報を原本情報として登録し、付与手段２は、その電子情報に対して、電子情報を論理的に一意に識別する論理識別情報と、電子情報の物理的所在を表す所在識別情報とを付与する。管理手段３は、論理識別情報と所在識別情報の組合せに基づく組合せ識別情報を用いて、原本情報を管理し、発行手段４は、その組合せ識別情報を含み、原本情報へのアクセスのために用いられる登録証書情報を発行する。

【０００８】登録手段１が登録する電子情報は、例えば、電子化された重要文書に対応し、登録された電子情報は、登録手段１内に保存される。また、電子情報の物理的所在は、例えば、登録手段１内で電子情報が保存されている場所（アドレス等）に対応する。管理手段３は、付与手段２により付与された論理識別情報と所在識別情報を組み合わせて組合せ識別情報を生成し、その組合せ識別情報を原本情報に付与する。そして、発行手段４は、その組合せ識別情報を含む登録証書情報を生成し、登録者等に発行する。

【０００９】電子情報を原本情報として登録し、付与手段２は、その電子情報に対して、電子情報を論理的に一意に識別する論理識別情報と、電子情報の物理的所在を表す所在識別情報とを付与する。管理手段３は、論理識別情報と所在識別情報の組合せに基づく組合せ識別情報を用いて、原本情報を管理し、発行手段４は、その組合せ識別情報を含み、原本情報へのアクセスのために用いられる登録証書情報を発行する。

【００１０】このような電子原本管理装置によれば、電子情報は登録されてはじめて原本情報として扱われるため、登録者側で生成された電子情報のコピーは原本情報ではないことを明確にすることができる。また、登録者および他の利用者は、発行された登録証書情報を用いて原本情報にアクセスするので、登録された原本情報を一意に識別することができる。したがって、原本管理の安全性が向上する。

【００１１】また、本発明の第２の局面において、管理手段３は、電子情報の時系列な変化に応じて、対応する原本情報の一連のインスタンスを生成し、その一連のインスタンスを１つの原本系列として管理する。付与手段２は、原本系列に対して原本系列識別情報を付与し、発行手段４は、その原本系列識別情報を含み、一連のインスタンスのうちの１つのインスタンスへのアクセスのために用いられる登録証書情報を発行する。

【００１２】原本情報のインスタンスは、登録された電子情報が更新等により変化した場合に生成され、管理手段３は、付与手段２により付与された原本系列識別情報を用いて、一連のインスタンスを管理する。そして、発行手段４は、その原本系列識別情報を含む登録証書情報を生成し、登録者等に発行する。

【００１３】このような電子原本管理装置によれば、更新等により刻々と生成される電子情報の系列を１つのグループとして扱うことができる。また、登録者および他の利用者は、発行された登録証書情報を用いて各インスタンスにアクセスするので、登録された原本系列を一意に識別することができる。したがって、原本管理の安全性が向上する。

【００１４】例えば、図１の登録手段１は、後述する図４の原本系列管理部３４と文書保管部３６に対応し、図１の付与手段２は、図４の物理ＩＤ作成部３７と識別Ｉ

Ｄ作成部４０に対応し、図１の管理手段３は、図４の原本系列管理部３４に対応し、図１の発行手段４は、図４の原本系列管理部３４と登録証書作成部３５に対応する。

【００１５】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態を詳細に説明する。本発明においては、利用者にサービスを提供するコンピュータ環境とは別に、電子原本管理装置を設ける。また、電子原本管理装置に登録される電子文書は、アプリケーションに依存した“原本”、“謄本”等の属性にかかわらず、すべて電子原本として扱われ、その電子原本に対して登録証書が発行される。すべて電子原本として扱うということは、電子文書を紙に出力した状態に対応し、以後、電子原本の利用者は、発行された登録証書を用いて電子原本にアクセスする。例えば、電子原本としては、次のようなものが登録される。

１．有価証券、健康保険証、紙幣等。原本を提示することによって権利や価値を示したり、原本の譲渡を行うことができる。

２．領収書等のように、商業活動で生成される文書（法廷文書）。原本を保管しておき、監査時等に証拠として提出することができる。

３．戸籍謄本、登記簿謄本等のように、契約書に添付される文書。戸籍謄本や登記簿謄本は、戸籍や登記簿の原本に登録されている内容と同じであることを保証し、契約時には、身元を保証する原本として契約書とともに保管される。

４．契約書等。同じ内容の契約書の原本を２部作成し、個々の原本を契約を交わした各当事者が保管する。

５．遺言書、契約書等。弁護士や公証人役場等の第３者をたてて、原本を第３者が保管し、その謄本を当事者たちが保管する。

６．議事録、企画書等のように、一般業務で生成される文書。これらの文書の原本を保管しておき、複数の当事者により共有する。

７．官公庁や地方自治体で生成される文書。保管機関や公開レベルを設定して管理する。

８．研究ノートや設計書等のように、特許紛争の際に証拠として提出される文書。

９．電子顕微鏡で撮ったＤＮＡ（deoxyribonucleic acid）の写真や、風洞実験の様子を写したフィルム等のように、研究の証拠となる画像情報。

【００１６】図２は、本実施形態において電子原本管理装置に保管される電子原本モデルを示している。図２において、セキュアアーカイバ（Secure Archiver，ＳＡ）は、電子原本管理装置に対応し、以下のような処理を行う。

Ｐ１：利用者側のコンピュータで処理され作成された電子文書は、ＳＡに登録されてはじめて電子原本となる。

このように、電子文書をＳＡに登録してはじめて原本として扱うことで、利用者側で電子文書のコピーが行われて全く同じ電子文書が作成されても、それらは原本ではなく、ＳＡ内の電子文書が原本であることを明確にすることができる。

Ｐ２：次に、ＳＡは、登録された電子文書（電子原本）に対して、登録証書を発行する。このように、ＳＡが登録証書を発行し、利用者が登録証書を用いてＳＡ内の電子原本にアクセスすることで、ＳＡ内の電子原本を一意に識別することが可能となる。

Ｐ３：次に、利用者側の同じ内容の電子文書をＳＡに二重登録しても、ＳＡ内では別々の原本として扱う。このように、ＳＡに登録される電子文書を別々の電子原本として扱うことで、紙媒体では同じ内容を印刷しても物理的に別々の物として扱うことが可能であったように、たとえ同じ内容であったとしても、電子的に各々独立した原本であると識別することが可能となる。

Ｐ４：次に、ある電子原本に対して更新が行われた際には、各時点の電子文書をその原本のインスタンスとして保持する。また、各々のインスタンスに対して、登録証書を発行する。このように処理することで、利用者は登録証書を用いて、ある原本のある時点のインスタンスを取り出すことが可能となる。

Ｐ５：Ｐ４で保持された一連のインスタンスを１つの原本として扱う。このように処理することで、更新等で状態が変化する原本を１つの原本として扱うことが可能となる。

Ｐ６：次に、ＳＡに登録されている電子原本からのコピーのみを電子原本のコピーとして扱う。このように処理することで、利用者側で発生するコピー文書と電子原本のコピーを明確に区別することが可能となる。

Ｐ７：次に、電子原本のオリジナルから作成されるコピーがどの時点の電子原本のコピーであるかを明確に区別する処理を行う。また、その電子原本のコピーに対して、登録証書を発行する。このように、どの時点の電子原本のコピーであるかを明確に示した登録証書を発行することで、利用者は、電子原本のコピーがどの時点のコピーであるかを明確に識別することが可能となる。

Ｐ８：次に、原本や謄本の属性等のアプリケーションから指定される登録情報と、コピーやオリジナル等の属性や作成日時等のＳＡが独自に管理する管理情報を電子文書と一体化して扱う。このように、アプリケーションとは独立して、電子文書、管理情報、および登録情報を一体化することで、たとえ文書が移動しても、移動先でその電子原本の属性を参照することが可能となる。

Ｐ９：次に、電子文書、管理情報、登録情報を一体化した形で改ざん検出情報（円で囲まれたＳＡにより表される部分）を作成する。このように、電子文書のみでなく、管理情報と登録情報をも含めて改ざん検出情報を作成することで、電子文書、管理情報、および登録情報の

整合性が保持される。

【００１７】図３は、上述したセキュアアーカイバを含む電子原本管理システムの構成図である。図３のシステムは、ＳＡ１１、サービスクライアント（利用者端末）１２、およびローカルな環境１３を含み、サービスクライアント１２とＳＡ１１の間と、２つのＳＡ１１間において、電子原本１４がやり取りされる。文書レコード１５は、図２の登録証書に対応し、ＳＡ１１内の電子原本１４へアクセスするために用いられる。

【００１８】サービスクライアント１２とＳＡ１１は、通信ネットワークに接続されており、サービスクライアント１２は、電子原本登録時にＳＡ１１から発行される文書レコード１５を用いて、ＳＡ１１内の電子原本１４にアクセスする。また、ＳＡ１１間のやり取りにおいては、ネットワーク接続の場合は、サービスクライアント１２とＳＡ１１の間の通信と同様に、文書レコード１５を用いて電子原本１４がやり取りされる。オフラインの場合は、セキュア媒体１６を用いて電子原本１４がやり取りされる。

【００１９】サービスクライアント側のローカルな環境１３は、会社内の１つの部署や事務所等で電子原本の唯一性等の安全性（原本性）を保証するシステムであり、ローカルＳＡ２１と利用者端末２２を含む。ローカルＳＡ２１内に管理されている電子原本は、ローカルな環境１３内のみで原本性が保証されており、他のＳＡ１１内の電子原本とはリンクしていない。ローカルＳＡ２１と外部のＳＡ１１の間では、通信ネットワークまたはセキュア媒体１６を介して、電子原本の情報をやり取りすることができる。

【００２０】図４は、図３のＳＡ１１の構成図である。図４のＳＡ１１は、ネットワークインタフェース３１、要求解釈部３２、返答作成部３３、原本系列管理部３４、登録証書作成部３５、文書保管部３６、物理ＩＤ作成部３７、暗号処理部３８、鍵保持部３９、識別ＩＤ作成部４０、時刻生成部４１、装置ＩＤ保持部４２、およびインクリメンタルカウンタ４３を備える。

【００２１】このうち、文書保管部３６と物理ＩＤ作成部３７は、ファイルシステムを構成し、暗号処理部３８、鍵保持部３９、識別ＩＤ作成部４０、時刻生成部４１、装置ＩＤ保持部４２、およびインクリメンタルカウンタ４３は、セキュリティハードウェアとして実装される。

【００２２】図５は、ＳＡ１１が行う処理のフローチャートである。ＳＡ１１の１つのトランザクションは、クライアント１２からの要求受信、要求に応じた装置内での処理、およびクライアント１２への返答送信からなる。まず、ネットワークインタフェース３１は、クライアント１２からの要求を受信し（ステップＳＴ１）、要求解釈部３２は、要求の種類を識別する（ステップＳＴ２）。

【００２３】次に、原本系列管理部３４は、各要求に従った処理を行い（ステップＳＴ３）、処理結果を作成する（ステップＳＴ４）。そして、返答作成部３３は、クライアント１２への返答メッセージを作成し（ステップＳＴ５）、ネットワークインタフェース３１は、クライアント１２へ返答メッセージを送信する（ステップＳＴ６）。これにより、１つのトランザクションが終了する。

【００２４】例えば、クライアント１２から文書の登録要求がくると、要求解釈部３２は、要求の種類が文書登録であると解釈し、クライアント１２から送付されてきた文書を原本系列管理部３４に渡す。

【００２５】次に、原本系列管理部３４は、暗号処理部３８を介して、識別ＩＤ作成部４０に論理識別ＩＤの作成を依頼し、文書保管部３６に文書を格納する。識別ＩＤ作成部４０は、時刻生成部４１からタイムスタンプを取得し、装置ＩＤ保持部４２からＳＡ１１の装置ＩＤを取得し、インクリメンタルカウンタ４３から装置内の文書ＩＤを表すカウンタ値を取得して、論理識別ＩＤを生成する。

【００２６】また、暗号処理部３８は、鍵保持部３９に保持されている装置鍵（ＳＡの個別鍵）を用いて、論理識別ＩＤにデジタル署名を施し、原本系列管理部３４に論理識別ＩＤを渡す。また、物理ＩＤ作成部３７は、文書の物理的な所在を表す物理ＩＤを作成し、文書保管部３６を介して原本系列管理部３４に渡す。

【００２７】原本系列管理部３４は、論理識別ＩＤと物理ＩＤを連結して暗号処理部３８に渡す。暗号処理部３８は、鍵保持部３９に保持されている装置鍵を用いて署名処理を行い、生成されたデジタルデータを識別ＩＤとして原本系列管理部３４に返す。原本系列管理部３４は、受け取った識別ＩＤを登録依頼された文書の識別情報として管理する。

【００２８】次に、原本系列管理部３４は、登録証書作成部３５に文書レコードの作成を指示し、登録証書作成部３５は、文書レコードを作成して原本系列管理部３４に返す。そして、原本系列管理部３４は、文書レコードを返答作成部３３に渡し、返答作成部３３は、クライアント１２への返答メッセージを作成し、ネットワークインタフェース３１を介してクライアント１２に送付して、処理を終了する。図３のＳＡ２１の構成についても同様である。

【００２９】次に、図６から図２６までを参照しながら、図３のシステムが行う処理をより詳細に説明する。上述したように、ＳＡは、電子原本の登録時に、登録証書として文書レコードを利用者に発行する。利用者は、文書レコードを用いてＳＡ内の電子原本にアクセスしたり、原本の共有者に文書レコードを送付したりする。共有者は、送付されてきた文書レコードを用いてＳＡにアクセスすることによって、原本を利用することができ

る。文書レコードの要件は、以下の通りである。
１．電子原本登録の事実を証明する。
２．ＳＡ内のどの原本に対して発行されたかを示す情報を提供する。
３．利用者のどの電子文書が原本として登録されたかを示す情報を提供する。
４．原本登録者（所有者）の情報を提供する。
５．アクセスすべきＳＡの情報を提供する。
６．文書レコードの改ざんを検出する。
【００３０】これらの要件から、ＳＡは、図６に示すような情報を文書レコードの中に埋め込んで発行する。電子原本のハッシュ値４１は、ＳＡに登録されている原本の内容をハッシュ関数により圧縮して得られた値である。このハッシュ値４１を利用者が持つ電子文書のハッシュ値と比較することによって、その電子文書が確かにＳＡに登録されている文書であることを確認することができる。したがって、ハッシュ値４１は、登録の事実を証明する情報として用いられる。ハッシュ値４１の代わりに、原本の内容を他の一方向性関数で変換した結果を用いてもよい。
【００３１】識別ＩＤ４２は、ＳＡ内の電子原本を一意に識別するための識別情報であり、論理識別ＩＤと物理ＩＤから生成される。ＳＡは、文書レコードがどの電子原本に対して発行されたのかを示す情報として、識別ＩＤを文書レコードに付加する。
【００３２】利用者側の電子文書名５３は、利用者側で管理しているファイル名に対応し、ＳＡ内の電子原本と利用者の電子文書を対応付ける情報として付加される。また、利用者ＩＤ５４は、原本登録時の認証に用いられる識別情報であり、原本の登録者（所有者）の情報として文書レコードに付加される。
【００３３】ＳＡの接続先情報５５は、ＳＡのＩＰ（Internet Protocol）アドレスやＦＱＤＮ（Fully Qualified Domain Name）等に対応し、アクセスすべきＳＡの識別情報として文書レコードに付加される。また、ＳＡの署名５６は、文書レコードの発行時に、文書レコードの情報に対してＳＡが計算して添付する署名情報であり、文書レコードをＳＡが発行したことを示すお墨付き情報でもある。利用者は、署名５６が添付された文書レコードをＳＡに送信し、電子文書の改ざんの有無を検証することができる。
【００３４】次に、原本系列の管理について説明する。ＳＡに登録された原本は、更新、移動、削除等の操作によりその状態が変化していく。ＳＡは、状態が変化するたびに、その時点の原本のインスタンスを保持し、一連のインスタンスを原本系列として管理する。そして、その原本系列に原本系列ＩＤを与えて、一意に識別する。これにより、サービスクライアントから見れば、その系列を１つの原本として特定し、取り出すことが可能となる。
【００３５】図７は、原本系列ＩＤにより原本系列を一意に識別する様子を示している。電子文書Ｄ１が電子文書Ｄ１－１としてＳＡに登録されると、ＳＡは、電子文書Ｄ１－１に原本系列ＩＤとしてＳＩＤ１を与え、原本系列Ｓ１として管理する。
【００３６】その後、電子文書Ｄ１に修正等が行われて原本の状態が変化し、再登録が行われると、ＳＡは、ＳＩＤ１を原本系列ＩＤとする電子文書Ｄ１－２のインスタンスを生成し、それを保持する。以後、状態変化が起こるたびに、電子文書Ｄ１－３、Ｄ１－４、Ｄ１－５のようなインスタンスが保持されていき、一連のインスタンスをＳＩＤ１により識別する。
【００３７】また、電子文書Ｄ１とは別に登録された電子文書Ｄ２には、新たに原本系列ＩＤとしてＳＩＤ２が与えられる。そして、電子文書Ｄ２の一連のインスタンスＤ２－１、Ｄ２－２、Ｄ２－３、Ｄ２－４、Ｄ２－５等は、ＳＩＤ２により識別され、原本系列Ｓ２として管理される。このとき、電子文書Ｄ２の内容が電子文書Ｄ１の内容とまったく同じでも、ＳＡは、各々を別の電子原本として管理する。
【００３８】このような原本系列ＩＤを用いれば、状態変化によって生成される一連のインスタンスを１つの原本として識別することが可能である。しかし、法廷文書の監査等を行う場合には、ある原本系列の中の任意の時点のインスタンスを特定して、取り出す必要がある。そのため、ＳＡは、原本系列の各時点のインスタンスにタイムスタンプを与える。
【００３９】図８は、ある原本系列の中で、時系列に変化するインスタンスをタイムスタンプによって管理している様子を示している。電子文書Ｄ１が電子文書Ｄ１－１として登録されると、登録時点のタイムスタンプＴ１が与えられ、以後、状態変化のたびに、各インスタンスにタイムスタンプＴ２、Ｔ３、Ｔ４、Ｔ５等が与えられる。利用者は、原本系列ＩＤとタイムスタンプを指定することにより、電子原本の任意の時点のインスタンスを特定して、取り出すことが可能となる。
【００４０】次に、電子原本のオリジナルとコピーの管理の要件を明確にするために、まず、電子文書のコピーの問題を明確にする。電子文書をコピーすると、オリジナルとまったく同じ電子文書が存在することになるため、コピーが氾濫し、どれが本物の原本であるか識別不可能となる。このため、従来は、媒体にラベルを貼る等の運用方法によりコピーが管理されていた。
【００４１】また、電子文書が不正にコピーされても、コピー元では、コピーされたことを識別することは不可能であり、また、コピー先では、コピーをオリジナルな電子文書として扱うことが可能となっている。なお、紙媒体の場合は、その質感からオリジナルとコピーを識別することができる。
【００４２】また、紙媒体の場合は、複数枚のコピーを

作成すると、各コピーを物理的に識別することが可能である。しかし、電子文書の場合は、オリジナルとまったく同じ内容のコピーとして存在するため、各コピーを識別することはおろか、オリジナルと区別することもできない。

【００４３】これらのことから、電子原本のオリジナルとコピーの管理には、以下のような要件が要求される。

１．電子原本のオリジナルとコピーを一意に指し示す手段を利用者に提供する。オリジナルとコピーを識別する情報を利用者に提供し、コピーがどの電子原本のオリジナルからのコピーであるかを識別可能にする。

２．複数回コピーをしても、各々のコピーを一意に識別可能である。

【００４４】これらの要件を満たすために、ＳＡは、次のようなオリジナルとコピーの管理を行う。

１．文書レコードによる電子原本のオリジナルとコピーの一意識別

ＳＡに電子文書を登録し、登録時に発行される文書レコードが指し示すＳＡ内の電子文書が原本であり、その電子原本のみから原本のコピーを生成するように管理する。また、コピー生成時にも文書レコードを発行し、その文書レコードが指し示すＳＡ内の電子文書のみを原本のコピーとして扱う。

【００４５】文書レコードが指し示す電子文書が電子原本あるいはそのコピーであるものとして管理することにより、たとえ、利用者側で文書レコードのコピーを行ったとしても、その文書レコードはＳＡ内の原本を一意に識別することが可能となる。したがって、どれが原本であるかわからないという問題やコピーの氾濫等の問題を解決することができる。

２．タイプ属性による管理

ＳＡに登録する電子原本に、オリジナルとコピーを識別する属性（タイプ属性）を与える。また、原本のコピー生成の際には、原本系列ＩＤとタイムスタンプを継承する電子文書を生成し、タイプ属性としてコピーを与え、この電子文書を原本のコピーとする。このようにして生成された電子原本のコピーは、どの電子原本のインスタンスから生成されたコピーであるかを明確に示している。タイプ属性は、文書レコードに付加されて利用者に通知され、利用者は文書レコードを参照することにより、電子原本のオリジナルとコピーを識別する。

【００４６】また、電子原本のコピーには、何回目のコピーかを示す追番を含むタイプ属性を与え、複数回コピーしたとしても、各々のコピーを独立した文書として識別可能にする。この追番は、文書レコードに付加されて利用者に通知され、利用者は個々の電子原本のコピーをそれぞれ独立したものとして識別する。こうして、追番を含むタイプ属性により、複数のコピーが管理される。

【００４７】図９は、電子原本のオリジナルとコピーを文書レコードを用いて一意に識別する様子を示している。電子文書Ｄ１が電子原本としてＳＡに登録されると、電子原本Ｏ１（オリジナル）としてＳＡ内に保持される。そして、その電子原本に対して、文書レコードＲ１（オリジナル）が発行される。

【００４８】この文書レコードＲ１は、ＳＡ内の電子原本Ｏ１を一意に識別する。また、この文書レコードＲ１が利用者のパーソナルコンピュータ等でコピーされたとしても、文書レコードＲ１のコピーはＳＡ内の電子原本Ｏ１を一意に指し示しているため、どれが本物の原本であるかわからなくなるという問題は生じない。

【００４９】次に、電子原本Ｏ１に対して、原本のコピーである電子原本Ｏ２（コピー）が生成されると、電子原本Ｏ２に対しても、電子原本Ｏ１と同様に、文書レコードＲ２が発行される。この文書レコードＲ２がコピーされたとしても、文書レコードＲ２のコピーはＳＡ内の電子原本Ｏ２を一意に識別することができる。

【００５０】なお、利用者側での電子文書Ｄ１のコピーは、通常のコピー操作であり、コピー先の電子文書Ｄ１－Ｃは原本としての効力を持たない。なぜなら、利用者のシステムでは、あくまでも、文書レコードＲ１が唯一に指し示すＳＡ内の電子文書を原本として管理しているからである。

【００５１】このような電子原本のオリジナルとコピーの管理によれば、たとえ、ＳＡ内の電子原本が不正に都合良く更新されたりしても、利用者のシステムは、ＳＡ内での原本の最新の状態や原本として有効なインスタンスを、文書レコードにより取り出すことができる。したがって、電子原本のオリジナルとコピーに対して、一意識別可能という安全性が与えられる。

【００５２】図１０は、電子文書にタイプ属性が割り振られる様子を示している。電子文書Ｄ１がＳＡに原本として登録される際、原本系列ＩＤとしてＳＩＤ１が与えられ、タイムスタンプとしてＴ１が与えられるとともに、タイプ属性としてオリジナルが与えられ、電子原本（オリジナル）として登録される。利用者がＳＡに登録する電子文書には、すべて、タイプ属性の初期値としてオリジナルが設定される。この登録時には、ＳＡは、電子原本の文書レコードＲ１（オリジナル）を利用者に対して発行する。

【００５３】そして、利用者が電子原本のコピー生成をＳＡに要求すると、ＳＡは、電子原本の原本系列ＩＤとタイムスタンプを継承し、タイプ属性をコピーに変更した電子原本（コピー）を新たに生成する。原本系列ＩＤとタイムスタンプを継承するのは、どの時点のインスタンスのコピーであるかを明確に識別するためである。そして、ＳＡは、電子原本（オリジナル）の場合と同様に、文書レコードＲ２（コピー）を利用者に発行する。

【００５４】図１１は、タイプ属性に与える追番により、複数存在する原本のコピーの各々を独立して管理し、利用者がそれらを一意に識別する様子を示してい

る。利用者が電子原本（オリジナル）のコピー生成を要求すると、ＳＡは、図９と同様の処理により、電子原本（コピー（１））を生成する。この時、タイプ属性のコピーには追番（１）が与えられる。

【００５５】利用者が、再度、電子原本のコピー生成を要求すると、電子原本（コピー（２））が生成され、タイプ属性のコピーに追番（２）が与えられる。また、利用者には、電子原本のコピー（１）、コピー（２）に対して、それぞれ、文書レコードＲ２、Ｒ３が発行される。このように、タイプ属性のコピーに追番を与えることにより、ＳＡ内で各々の電子原本のコピーを独立に管理することが可能となる。また、利用者は、文書レコードを用いて、各々の電子原本のコピーを一意に識別することが可能となる。

【００５６】次に、文書の物理的な所在の管理について説明する。紙媒体は、移動すると元の場所からなくなってしまうため、原本が物理的にどこにあるかを認識することは可能である。しかし、原本管理簿等で原本の所在を管理しても、その原本があるべき場所（所在）を保証することができなかった。電子文書も紙媒体と同様に、以下のような問題を持っている。

１．電子文書の所在を一意に特定できない。

２．コピーや移動が簡単に行うことが可能なため、不正コピーや盗難を検出することができない。

【００５７】そこで、ＳＡは、電子原本に対して以下のような処理を行い、電子原本の所在を保証する。

１．ＳＡに登録する電子原本に、物理的に所在を特定する情報（物理ＩＤ）を与えて、所在を一意に特定する。

２．物理ＩＤを用いて不正コピーの検出を行う。

【００５８】ネットワークやオフラインシステムが混在する環境において、複数のＳＡが電子原本を管理することが予想される。そこで、物理ＩＤは、ＳＡを特定するＳＡ－ＩＤとＳＡ内のどの媒体のどの位置に保管しているかを示すアドレスＩＤから構成する。アドレスＩＤとしては、例えば、媒体上の物理アドレスが用いられる。

【００５９】図１２は、物理ＩＤにより電子原本の所在を特定し、不正コピーを検出する様子を示している。電子文書Ｄ１の物理ＩＤであるＰＩＤ１は、ＳＡ－ＩＤと文書保管部３６のアドレスＩＤ（ＡＩＤ１）から構成され、その物理ＩＤが電子文書Ｄ１に付加されている。電子文書Ｄ２と電子文書Ｄ３は、それぞれ、ＡＩＤ２とＡＩＤ３をアドレスＩＤとして正常に保管されている電子原本である。

【００６０】物理ＩＤのテーブルは、図４の物理ＩＤ作成部３７に保持され、各電子文書とそのアドレスＩＤから生成された物理ＩＤの対応関係を格納している。電子文書Ｄ１、Ｄ２、Ｄ３の物理ＩＤは、それぞれ、ＰＩＤ１、ＰＩＤ２、ＰＩＤ３である。

【００６１】ここで、管理者等が電子文書Ｄ１を不正にコピーすると、コピーの電子文書Ｄ１－Ｃは、ＡＩＤ４をアドレスＩＤとする場所に保管される。この場合、電子文書Ｄ１－Ｃが持つ物理ＩＤはＰＩＤ１であり、物理ＩＤのテーブルに登録される物理ＩＤはＳＡ－ＩＤとＡＩＤ４から構成されるＰＩＤ４である。したがって、両者の物理ＩＤを比較すれば、それらが異なることがわかり、不正コピーが検出される。なお、別のＳＡに不正コピーされた場合には、ＳＡ－ＩＤが異なるため、同様にして不正コピーが検出される。

【００６２】次に、図１３は、原本系列における各種識別情報の変化の例を示している。図１３では、以下のような手順で識別情報が変更される。

Ｐ１：登録

時刻Ｔ１において、利用者は、ＳＡ１に電子文書Ｄ１－１を登録する。ＳＡ１は、登録の処理として、第１に、ＳＩＤ１を原本系列ＩＤとして割り振る。この原本系列ＩＤにより、原本の状態の変化していく系列が一意に識別される。第２に、タイムスタンプとしてＴ１を割り振る。このタイムスタンプにより、原本系列での各時点のインスタンスが一意に識別される。第３に、タイプ属性としてオリジナルを設定する。ＳＡに登録される電子文書のタイプ属性は、すべて、オリジナルである。

【００６３】そして、ＳＡ１は、これらの識別情報、すなわち、原本系列ＩＤ、タイムスタンプ、およびタイプ属性により、各時点での原本を論理的に一意に識別する。また、第４に、物理ＩＤとしてＰＩＤ１を割り振る。この物理ＩＤにより、電子文書の所在を明確にし、不正コピーの検出等を行う。

Ｐ２：更新（状態変化）

時刻Ｔ２において、利用者は、電子文書Ｄ１－１を更新し、電子文書Ｄ１－２を生成する。これにより、原本の状態が変化する。このとき、原本系列ＩＤとタイプ属性は変更されず、新たなタイムスタンプと物理ＩＤとして、それぞれ、Ｔ２とＰＩＤ２が割り振られた電子原本が作成される。

Ｐ３：コピー作成

利用者は、電子文書Ｄ１－２のコピーを作成する。このとき、原本系列ＩＤとタイムスタンプは変更されず、新たなタイプ属性と物理ＩＤとして、それぞれ、コピー（１）とＰＩＤ３が割り振られた電子原本が作成される。タイムスタンプを変更しないのは、原本系列のある時点のコピーであることを明確に識別するためである。コピーを作成した時刻は、履歴等の管理情報として保持される。また、コピー属性には追番が振られ、個々のコピーのインスタンスが管理される。

Ｐ４：移動

時刻Ｔ３において、利用者は、電子文書Ｄ１－２をＳＡ１からＳＡ２に移動する。このとき、原本系列ＩＤとタイプ属性は変更されず、新たなタイムスタンプと物理ＩＤとして、それぞれ、Ｔ３とＰＩＤ４が割り振られた電子原本が作成される。物理ＩＤにはＳＡを一意に識別す

るＩＤが含まれているので、これを用いて不当な電子文書の移動を検出することができる。

【００６４】次に、ＳＡ内で行われる処理についてより詳細に説明する。図１４は、識別ＩＤの生成の様子を示している。ここでは、以下のような手順で処理が行われる。

Ｐ１：論理識別ＩＤ作成要求

電子文書の登録要求を受けると、原本系列管理部３４は、論理識別ＩＤ作成要求をセキュリティハードウェアに対して行う。

Ｐ２：要求

要求時に、原本系列管理部３４は、オリジナル原本に対する要求か、コピー原本に対する要求かを指定するタイプ属性をセキュリティハードウェアに対して与える。また、コピー原本の場合には、コピー元のオリジナル原本の論理識別ＩＤも与える。

Ｐ３：論理識別ＩＤ生成

セキュリティハードウェアは、図４の暗号処理部３８、鍵保持部３９、識別ＩＤ作成部４０、時刻生成部４１、装置ＩＤ保持部４２、およびインクリメンタルカウンタ４３を含む。

【００６５】識別ＩＤ作成部４０は、装置ＩＤ保持部４２が保持している装置ＩＤとインクリメンタカウンタ４３が保持しているカウンタ値から原本系列ＩＤ６１を生成し、時刻生成部４１内のリアルタイムクロック（ＲＴＣ）が出力する時刻からタイムスタンプ６３を生成する。そして、これらの情報を原本系列管理部３４が指定したタイプ属性６２と連結して、論理識別ＩＤを生成する。コピー原本の場合には、与えられたオリジナル原本の論理識別ＩＤに含まれる原本系列ＩＤとタイムスタンプを継承して、論理識別ＩＤを生成する。

Ｐ４：ＳＡの署名

暗号処理部３８は、鍵保持部３９に保持されているＳＡの個別鍵６４を用いて、Ｐ３で連結された情報に対してＳＡのデジタル署名を生成する。ＳＡのデジタル署名は、ＳＡの個別鍵６４で作成するＭＡＣ（Message Authentication Code）に対応する。暗号処理部３８は、Ｐ３で連結された情報にこのＭＡＣの値を連結して、電子文書を論理的に識別する最終的な論理識別ＩＤ６６を生成する。図１４において、円で囲まれたＳＡは、生成された情報がＳＡのデジタル署名を含むことを表している。

Ｐ５：論理識別ＩＤ返答

暗号処理部３８は、論理識別ＩＤ６６を、論理識別ＩＤ作成要求に対するセキュリティハードウェアの処理結果として、原本系列管理部３４に返す。

Ｐ６：電子文書保管

ファイルシステムは、文書保管部３６と物理ＩＤ作成部３７を含む。原本系列管理部３４は、返された論理識別ＩＤ６６をファイル名として、電子文書をファイルシステム内の文書保管部３６に格納する。

Ｐ７：識別ＩＤ作成要求

原本系列管理部３４は、識別ＩＤ作成要求をセキュリティハードウェアに対して行う。このとき、物理ＩＤ作成部３７から物理ＩＤ６７を取得し、論理識別ＩＤ６６と物理ＩＤ６７をセキュリティハードウェアに与える。

Ｐ８：ＳＡの署名

暗号処理部３８は、ＳＡの個別鍵６４を用いて、論理識別ＩＤ６６と物理ＩＤ６７を連結した情報に対してＳＡの署名を生成する。そして、論理識別ＩＤ６６と物理ＩＤ６７を連結した情報にＳＡの署名を連結して、識別ＩＤ６８を生成する

Ｐ９：識別ＩＤ返答

暗号処理部３８は、識別ＩＤ作成要求に対するセキュリティハードウェアの処理結果として、識別ＩＤ６８を返す。

Ｐ１０：識別ＩＤを管理情報に格納

識別ＩＤ６８を電子原本の管理情報として格納する。

【００６６】図１５は、ＳＡ内で電子文書を保管する様子を示している。ここでは、以下のような手順で処理が行われる。

Ｐ１：原本系列管理部３４は、クライアントから電子文書７１と登録情報７２を取得し、セキュリティハードウェアに識別ＩＤの生成を指示する。登録情報７２には、利用者ＩＤと利用者の電子文書名が含まれる。

Ｐ２：セキュリティハードウェアは、識別ＩＤ６８を生成して、原本系列管理部３４に返す。

Ｐ３：原本系列管理部３４は、電子文書７１、登録情報７２、および管理情報７３を識別ＩＤ６８に関連付け、これらの情報を連結する。管理情報７３には、ＳＡの接続先情報が含まれる。

Ｐ４：原本系列管理部３４は、セキュリティハードウェアに改ざん検出情報の生成を指示する。このとき、電子文書７１、登録情報７２、および管理情報７３を連結した情報を、セキュリティハードウェアに与える。

Ｐ５：セキュリティハードウェアは、受け取った情報に対して、ＳＡの個別鍵６４を用いてＳＡの署名を生成する。そして、それを改ざん検出情報として管理情報に付加し、電子原本７４を生成する。

Ｐ６：セキュリティハードウェアは、電子原本７４を処理結果として返す。

Ｐ７：原本系列管理部３４は、電子原本７４を原本のオリジナルとして、ファイルシステムに登録する。

【００６７】図１６は、文書レコード生成の様子を示している。ここでは、以下のような手順で処理が行われる。

Ｐ１：文書レコード情報整形

原本系列管理部３４は、電子原本７４の管理情報から、識別ＩＤとＳＡの接続先情報を取得し、電子原本７４の登録情報から、利用者ＩＤと利用者の電子文書名を取得

して、取得した情報を図４の登録証書作成部３５に渡す。登録証書作成部３５は、受け取った情報を文書レコード情報８１として整形し、原本系列管理部３４に返す。

Ｐ２：文書レコード作成指示

原本系列管理部３４は、電子文書７１と文書レコード情報８１をセキュリティハードウェアに与えて、文書レコードの作成を指示する。

Ｐ３：ハッシュ値計算

セキュリティハードウェア内の暗号処理部３８は、電子文書７１のハッシュ値８２を計算する。

Ｐ４：ハッシュ値連結

暗号処理部３８は、ハッシュ値８２を文書レコード情報８１に連結する。

Ｐ５：改ざん検出情報生成

暗号処理部３８は、図１５の処理と同様に、ＳＡの個別鍵６４を用いて改ざん検出情報を生成し、改ざん検出情報を文書レコード情報８１に連結して、文書レコード８３を生成する。

Ｐ６：文書レコード返答

暗号処理部３８は、文書レコード８３を処理結果として原本系列管理部３４に返す。

Ｐ７：原本系列管理部３４は、文書レコード８３をクライアントに送信する。

【００６８】次に、ＳＡの基本機能である登録、検索、文書レコード検証、同一性検証、更新、移動、チェックアウト・チェックイン、および状態遷移取得について説明する。

【００６９】図１７は、電子文書の登録の様子を示している。登録とは、クライアントが生成した電子文書をＳＡに原本として登録することである。ここでは、以下のような手順で処理が行われる。

Ｐ１：クライアントは、ファイル名９１の電子文書７１を作成し、社外秘等の属性や保管期間のように、サービスに依存する情報を登録情報７２として作成する。

Ｐ２：クライアントは、ファイル名９１、電子文書７１、および登録情報７２を、クライアントとＳＡの間のセッション鍵で暗号化して、ＳＡに送信する。図１７において、円で囲まれた文字“セ”は、情報がセッション鍵により暗号化されていることを表している。

Ｐ３：ＳＡは、受け取った情報を復号化し、電子文書７１に対して、識別ＩＤと、作成日時や改ざん検出情報等を含む管理情報を自動生成し、生成した情報を電子文書７１および登録情報７２と連結して、原本のオリジナル７４を生成する。

Ｐ４：ＳＡは、登録の結果として、文書レコード８３を発行する。文書レコード８３には、図１６に示したような情報が含まれている。このうち、ＳＡの接続先情報としては、例えば、ＳＡのエイリアス（alias）名が用いられる。基本的には、この文書レコード８３を用いて他の処理が行われる。

Ｐ５：ＳＡは、文書レコード８３をセッション鍵で暗号化して、クライアントに通知する。

Ｐ６：クライアントは、受け取った情報を復号化し、ファイル名９１に文書レコード８３を関連付けて、情報を更新する。

【００７０】図１８は、電子文書の検索（参照）の様子を示している。検索とは、ＳＡに保管されている電子文書を文書レコードの情報（識別ＩＤ）をキーとして取り出すことである。ここでは、以下のような手順で処理が行われる。

Ｐ１：クライアントは、検索対象の電子文書の文書レコード８３を選択し、接続先情報からアクセスするＳＡを確認する。

Ｐ２：クライアントは、文書レコード８３をＳＡに送付する。

Ｐ３：ＳＡは、文書レコード８３の識別ＩＤをキーとして、原本７４を検索する。

Ｐ４：ＳＡは、検索された原本７４の電子文書をクライアントに通知する。

Ｐ５：クライアントは、受け取った電子文書をファイル名９１に関連付けて、情報を更新する。

【００７１】図１９は、文書レコードの検証の様子を示している。文書レコード検証とは、クライアントに保持されている文書レコードが最新のものであるか否かを検証することである。図１９では、ＳＡ内の電子原本の状態が更新等により変化しており、最新の文書レコードが新たに通知されている。ここでは、以下のような手順で処理が行われる。

Ｐ１：クライアントは、検証対象の電子文書を選択する。ここでは、ファイル名９２の電子文書９３が選択されている。

Ｐ２：クライアントは、電子文書９３の文書レコード９４をＳＡに送付する。

Ｐ３：ＳＡは、クライアントから送られてきた文書レコード９４の識別ＩＤから原本系列ＩＤを取り出し、その原本系列ＩＤに対応する原本系列の中でタイムスタンプが最新の電子原本９５を検索する。そして、電子原本９５の識別ＩＤと文書レコード９４の識別ＩＤを比較する。両者が一致すれば、文書レコード９４は最新のものであることがわかり、両者が一致しなければ、電子原本の状態が変化していることがわかる。

Ｐ４：ＳＡは、電子原本の状態が変化していることを検出し、最新の文書レコード９６を作成する。

Ｐ５：ＳＡは、最新の文書レコード９６をクライアントに通知する。

Ｐ６：クライアントは、通知された文書レコード９６をファイル名９１に関連付け、情報を更新する。その後、最新の電子文書を取得する場合には、文書レコード９６を用いて、図１８の検索処理により電子文書を取得す

る。

【００７２】図２０は、同一性検証の様子を示している。同一性検証とは、クライアントが保存している電子文書とＳＡ内の電子原本とが同一であるか否かを検証することである。ここでは、以下のような手順で処理が行われる。

Ｐ１：クライアントは、検証対象の電子文書９３と文書レコード９４を選択する。

Ｐ２：クライアントは、文書レコード９４と電子文書９３をＳＡに送付する。

Ｐ３：ＳＡは、クライアントから送られてきた電子文書９３の改ざん検出情報を計算し、文書レコード９４が指し示すＳＡ内の電子原本９７の改ざん検出情報と比較して、両者が同一か否かを検証する。

Ｐ４：ＳＡは、検証結果９８に署名を行って、クライアントに通知する。

Ｐ５：クライアントは、検証結果９８を確認する。

【００７３】図２１は、電子文書の更新の様子を示している。更新とは、ＳＡ内の電子文書に対応するクライアント内の電子文書を、更新文書としてＳＡ内の電子文書に関連付けることである。ここでは、以下のような手順で処理が行われる。

Ｐ１：クライアントは、更新文書として電子文書Ｄ２を作成し、更新対象の電子文書Ｄ１の文書レコードＲ１、電子文書Ｄ２、および電子文書Ｄ２に関わる登録情報Ｇ２を選択する。

Ｐ２：クライアントは、文書レコードＲ１、電子文書Ｄ２、および登録情報Ｇ２をＳＡに送付する。

Ｐ３：ＳＡは、文書レコードＲ１に対応する電子原本Ｏ１を取得し、その識別ＩＤであるＩＤ１のタイムスタンプ部分を更新して、新たな識別ＩＤとしてＩＤ２を生成する。そして、電子文書Ｄ２をＩＤ２に関連付けて登録し、電子原本Ｏ２を生成する。このとき、電子原本Ｏ１の管理情報Ｍ１、登録情報Ｇ１は更新されて、それぞれ、管理情報Ｍ２、登録情報Ｇ３となる。登録情報Ｇ３は、登録情報Ｇ１と登録情報Ｇ２を含む。

Ｐ４：ＳＡは、更新された電子原本Ｏ２の文書レコードＲ２を作成する。

Ｐ５：ＳＡは、文書レコードＲ２をクライアントに通知する。

Ｐ６：クライアントは、文書レコードＲ２を電子文書Ｄ２のファイル名に関連付けて、情報を更新する。

【００７４】図２２および図２３は、電子文書の移動の様子を示している。移動とは、ＳＡ内の電子文書を他のＳＡに移動することである。移動元の電子文書の情報は、サービス形態に応じて、残される場合と消去される場合とがある。ここでは、移動元の電子文書の情報を残すものとし、以下のような手順で処理が行われる。

Ｐ１：クライアントは、移動する電子文書Ｄ１と移動先ＳＡを選択する。移動先ＳＡのリストは、必要に応じて、移動元ＳＡから示される。

Ｐ２：クライアントは、電子文書Ｄ１の文書レコードＲ１と移動先ＳＡを指定する情報１０１を、移動元ＳＡに送付する。

Ｐ３：移動元ＳＡは、文書レコードＲ１が指し示す電子原本Ｏ１の電子文書Ｄ１に対するエキスポート処理を行う。まず、識別ＩＤがＩＤ１である電子文書Ｄ１、管理情報Ｍ１、および登録情報Ｇ１を連結する。次に、連結データに対して、移動先ＳＡと移動元ＳＡが共有している共通鍵（個別共有鍵、グループ共有鍵等）を用いて、改ざん検出情報を生成する。そして、改ざん検出情報を元の連結データと連結して、パックドデータ１０２を生成する。

Ｐ４：移動元ＳＡは、パックドデータ１０２を移動先ＳＡに送付する。

Ｐ５：移動先ＳＡは、パックドデータ１０２の改ざんの有無を検証し、インポート処理を行う。この処理では、パックドデータ１０２をアンパックして、電子文書Ｄ１、管理情報Ｍ１、および登録情報Ｇ１を取り出す。

Ｐ６：移動先ＳＡは、ＩＤ１のタイムスタンプと物理ＩＤを更新して、タイムスタンプと物理ＩＤが異なる識別ＩＤであるＩＤ２を生成する。

Ｐ７：移動先ＳＡは、３ウェイハンドシェークによる否認防止の処理として、否認防止レコード１０３とＩＤ２を移動元ＳＡに送付する。

Ｐ８：移動元ＳＡは、受け取ったＩＤ２のタイムスタンプを更新してＩＤ３を生成し、ＩＤ３に関連付けて、電子文書Ｄ１のハッシュ値１０４を移動した電子文書の情報（電子原本Ｏ３）として登録する。電子原本Ｏ３には、移動先の識別ＩＤであるＩＤ２が付加された管理情報Ｍ３と、登録情報Ｇ１が含まれる。

Ｐ９：移動元ＳＡは、３ウェイハンドシェークによる否認防止の処理として、否認防止レコード１０３を移動先ＳＡに送付する。

Ｐ１０：移動先ＳＡは、ＩＤ２に関連付けて、電子文書Ｄ１を移動してきた電子文書（電子原本Ｏ２）として登録する。電子原本Ｏ２には、移動元の識別ＩＤであるＩＤ１が付加された管理情報Ｍ２と、登録情報Ｇ１が含まれる。

Ｐ１１：移動元ＳＡは、ＩＤ２の情報を含む文書レコードＲ３を生成する。

Ｐ１２：移動元ＳＡは、文書レコードＲ３をクライアントに送信する。

Ｐ１３：移動先ＳＡは、ＩＤ１の情報を含む文書レコードＲ２を生成する。

Ｐ１４：移動先ＳＡは、文書レコードＲ２をクライアントに送信する。

Ｐ１５：クライアントは、文書レコードＲ２、Ｒ３を電子文書Ｄ１のファイル名に関連付け、情報を更新する。

【００７５】図２４は、チェックアウトおよびチェック

インの様子を示している。チェックアウトとは、利用者からの要求により、ＳＡ内に登録されている原本をロックし、チェックイン要求があるまで原本の状態を変化させないようにすることである。また、チェックインとは、利用者からの要求により、原本のロックを解除することである。ここでは、以下のような手順で処理が行われる。

Ｐ１：クライアントは、チェックアウト対象の電子文書Ｄ１を選択する。

Ｐ２：クライアントは、電子文書Ｄ１の文書レコードＲ１をＳＡに送付して、チェックアウトを要求する。

Ｐ３：ＳＡは、チェックアウト処理を行う。まず、電子文書Ｄ１を含む電子原本Ｏ１の管理情報Ｍ１にチェックアウト属性を付与し、識別ＩＤであるＩＤ１のタイムスタンプを更新して、タイムスタンプが異なるＩＤ２を生成する。そして、チェックアウト属性を有する文書レコードＲ２を作成する。

Ｐ４：ＳＡは、文書レコードＲ２をクライアントに通知する。

Ｐ５：クライアントは、電子文書Ｄ１を電子文書Ｄ２に更新する。この更新処理は、クライアント内だけではなく、更新機能を用いて、ＳＡ内のＩＤ２の電子文書に対して行うこともできる。また、更新処理は、複数回行ってもよい。

Ｐ６：クライアントは、文書レコードＲ２、最終的な電子文書Ｄ２、電子文書Ｄ２の登録情報Ｇ２をＳＡに送付して、チェックインを要求する。

Ｐ７：ＳＡは、チェックイン処理を行う。まず、ＩＤ２のタイムスタンプを更新してＩＤ３を生成し、管理情報Ｍ１にチェックイン属性を付与して管理情報Ｍ２を生成する。そして、電子文書Ｄ２を電子原本Ｏ２として登録する。

Ｐ８：ＳＡは、チェックイン属性を有する文書レコードＲ３を作成する。

Ｐ９：ＳＡは、文書レコードＲ３をクライアントに通知する。

Ｐ１０：クライアントは、文書レコードＲ３を電子文書Ｄ２のファイル名に関連付けて、情報を更新する。

【００７６】図２５は、状態遷移取得の様子を示している。状態遷移取得とは、文書レコードが指す電子原本の状態がどのように遷移したかを示す状態遷移情報を取得することである。状態遷移情報は、電子原本に対して行われた操作の履歴に対応し、管理情報の一部として保持される。ここでは、以下のような手順で処理が行われる。

Ｐ１：クライアントは、状態遷移情報を取得すべき電子文書９３を選択する。

Ｐ２：クライアントは、電子文書９３の文書レコード９４をＳＡに送付する。

Ｐ３：ＳＡは、文書レコード９４が指し示すＳＡ内の電子原本９７の最新の管理情報から、状態遷移情報１０５を取得する。

Ｐ４：ＳＡは、状態遷移情報１０５をクライアントに通知する。

Ｐ５：クライアントは、状態遷移情報１０５の内容を確認する。

【００７７】図２６は、状態遷移情報の例を示している。この状態遷移情報には、１９９８年2月１７日の１２：００に、ユーザＡがＳＡ１に原本を登録し、１４：００に、ユーザＢがＳＡ１からＳＡ２に原本を移動し、１５：００に、ユーザＣが原本のコピーを作成し、１６：００に、ユーザＤがＳＡ２からＳＡ３に原本を移動したことが記録されている。したがって、利用者は、状態遷移情報を参照することで、登録時から現在までの電子原本の状態を追跡することができる。

【００７８】以上説明した実施形態では、主として、電子化された重要文書を電子文書としてＳＡに登録しているが、それ以外にも、任意のフォーマットの任意の電子情報をＳＡに登録することが可能である。例えば、音声データ、画像データ、ビデオデータ等を登録しておき、電子文書と同様にして管理することができる。

【００７９】ところで、図３のＳＡ１１、２１、クライアント１２、および端末２２は、例えば、図２７に示すような情報処理装置（コンピュータ）を用いて構成することができる。図２７の情報処理装置は、ＣＰＵ（中央処理装置）１１１、メモリ１１２、入力装置１１３、出力装置１１４、外部記憶装置１１５、媒体駆動装置１１６、およびネットワーク接続装置１１７を備え、それらはバス１１８により互いに接続されている。

【００８０】メモリ１１２は、例えば、ＲＯＭ（read only memory）、ＲＡＭ（random access memory）等を含み、処理に用いられるプログラムとデータを格納する。例えば、図４に示した原本系列管理部３４と登録証書作成部３５は、プログラムモジュールとしてメモリ１１２に格納される。ＣＰＵ１１１は、メモリ１１２を利用してプログラムを実行することにより、必要な処理を行う。

【００８１】入力装置１１３は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、利用者または管理者からの指示や情報の入力に用いられる。出力装置１１４は、例えば、ディスプレイ、プリンタ、スピーカ等であり、利用者または管理者への問い合わせや処理結果の出力に用いられる。

【００８２】外部記憶装置１１５は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク（magneto-optical disk）装置等である。情報処理装置は、この外部記憶装置１１５に、上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ１１２にロードして使用することができる。また、外部記憶装置１１５は、図４の文書保管部３６および物理ＩＤ作成部３７

としても用いられる。

【００８３】媒体駆動装置１１６は、可搬記録媒体１１９を駆動し、その記録内容にアクセスする。可搬記録媒体１１９としては、メモリカード、フロッピーディスク、ＣＤ－ＲＯＭ（compact disk read only memory）、光ディスク、光磁気ディスク等、任意のコンピュータ読み取り可能な記録媒体が用いられる。利用者は、この可搬記録媒体１１９に上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ１１２にロードして使用することができる。また、可搬記録媒体１１９は、図３のセキュア媒体１６としても用いられる。

【００８４】ネットワーク接続装置１１７は、ＬＡＮ（local area network）等の任意のネットワーク（回線）を介して外部の装置と通信し、通信に伴うデータ変換を行う。情報処理装置は、必要に応じて、上述のプログラムとデータをネットワーク接続装置１１７を介して外部の装置から受け取り、それらをメモリ１１２にロードして使用することができる。ネットワーク接続装置１１７は、例えば、図４のネットワークインタフェース３１に対応する。

【００８５】図２８は、図２７の情報処理装置にプログラムとデータを供給することのできるコンピュータ読み取り可能な記録媒体を示している。可搬記録媒体１１９や外部のデータベース１２０に保存されたプログラムとデータは、メモリ１１２にロードされる。そして、ＣＰＵ１１１は、そのデータを用いてそのプログラムを実行し、必要な処理を行う。

【００８６】

【発明の効果】本発明によれば、利用者が利用するコンピュータ環境とは別に、電子原本管理装置を設け、電子原本管理装置が発行する登録証書を用いて、電子文書の登録、更新、移動等の処理が行われる。これにより、電子文書に対して、紙媒体と同等以上の安全性（原本性）を与えることが可能となる。

【図面の簡単な説明】

【図１】本発明の電子原本管理装置の原理図である。

【図２】電子原本モデルを示す図である。

【図３】電子原本管理システムの構成図である。

【図４】セキュアアーカイバの構成図である。

【図５】セキュアアーカイバの処理のフローチャートである。

【図６】文書レコードを示す図である。

【図７】原本系列の管理を示す図である。

【図８】時系列管理を示す図である。

【図９】オリジナルとコピーの識別を示す図である。

【図１０】タイプ属性による管理を示す図である。

【図１１】複数コピーの管理を示す図である。

【図１２】不正コピーの検出を示す図である。

【図１３】識別情報の変化を示す図である。

【図１４】識別ＩＤの生成を示す図である。

【図１５】電子文書の保管を示す図である。

【図１６】文書レコードの生成を示す図である。

【図１７】登録処理を示す図である。

【図１８】検索処理を示す図である。

【図１９】文書レコード検証処理を示す図である。

【図２０】同一性検証処理を示す図である。

【図２１】更新処理を示す図である。

【図２２】移動処理を示す図（その１）である。

【図２３】移動処理を示す図（その２）である。

【図２４】チェックアウト・チェックイン処理を示す図である。

【図２５】状態遷移取得処理を示す図である。

【図２６】状態遷移情報を示す図である。

【図２７】情報処理装置の構成図である。

【図２８】記録媒体を示す図である。

【符号の説明】

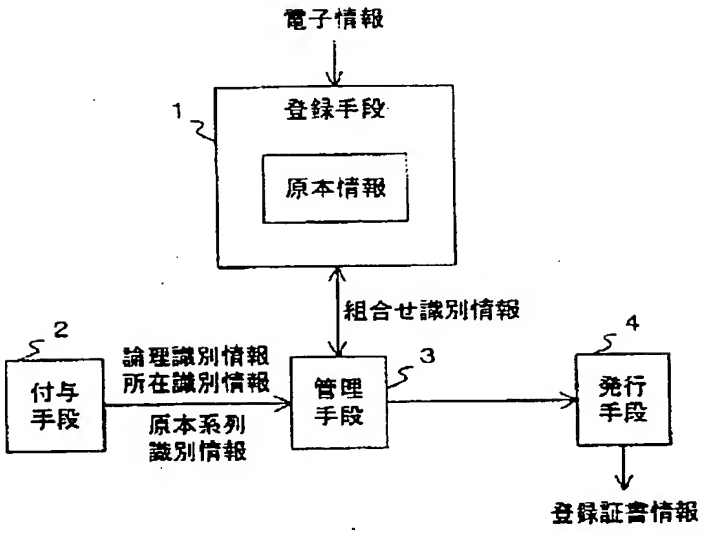
１　登録手段
２　付与手段
３　管理手段
４　発行手段
１１、２１　セキュアアーカイバ
１２　サービスクライアント
１３　ローカルな環境
１４、７４、９５、９７、Ｏ１、Ｏ２、Ｏ３　電子原本
１５、８３、９４、９６、Ｒ１、Ｒ２、Ｒ３　文書レコード
１６　セキュア媒体
２２　利用者端末
３１　ネットワークインタフェース
３２　要求解釈部
３３　返答作成部
３４　原本系列管理部
３５　登録証書作成部
３６　文書保管部
３７　物理ＩＤ作成部
３８　暗号処理部
３９　鍵保持部
４０　識別ＩＤ作成部
４１　時刻生成部
４２　装置ＩＤ保持部
４３　インクリメンタルカウンタ
５１、８２、１０４　ハッシュ値
５２、６８　識別ＩＤ
５３　利用者側の電子文書名
５４　利用者ＩＤ
５５　ＳＡの接続先情報
５６　ＳＡの署名
６１、ＳＩＤ１、ＳＩＤ２　原本系列ＩＤ
６２　タイプ属性

25　　26

６３　Ｔ１、Ｔ２、Ｔ３、Ｔ４、Ｔ５　タイムスタンプ
６４　ＳＡの個別鍵
６６　論理識別ＩＤ
６７、ＰＩＤ１、ＰＩＤ２、ＰＩＤ３、ＰＩＤ４　物理ＩＤ
７１、９３、Ｄ１、Ｄ１－１、Ｄ１－２、Ｄ１－３、Ｄ１－４、Ｄ１－５、Ｄ１－Ｃ、Ｄ２、Ｄ２－１、Ｄ２－２、Ｄ２－３、Ｄ２－４、Ｄ２－５　電子文書
７２、Ｇ１、Ｇ２、Ｇ３　登録情報
７３、Ｍ１、Ｍ２、Ｍ３　管理情報
８１　文書レコード情報
９１、９２　ファイル名
９８　検証結果
１０１　移動先ＳＡの情報
１０２　パックドデータ
１０３　否認防止レコード
１０５　状態遷移情報
１１１　ＣＰＵ
１１２　メモリ
１１３　入力装置
１１４　出力装置
１１５　外部記憶装置
１１６　媒体駆動装置
１１７　ネットワーク接続装置
１１９　可搬記録媒体
１２０　データベース
Ｓ１、Ｓ２　原本系列
ＡＩＤ１、ＡＩＤ２、ＡＩＤ３、ＡＩＤ４　アドレスＩＤ

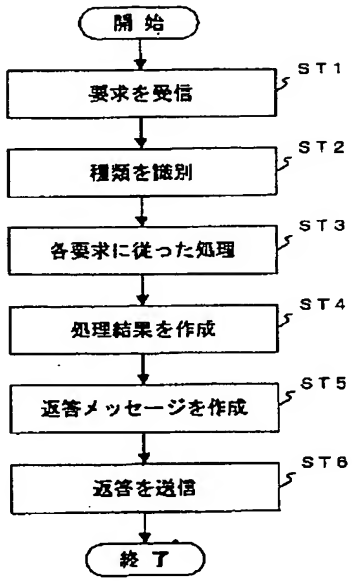
【図１】

本　発　明　の　原　理　図



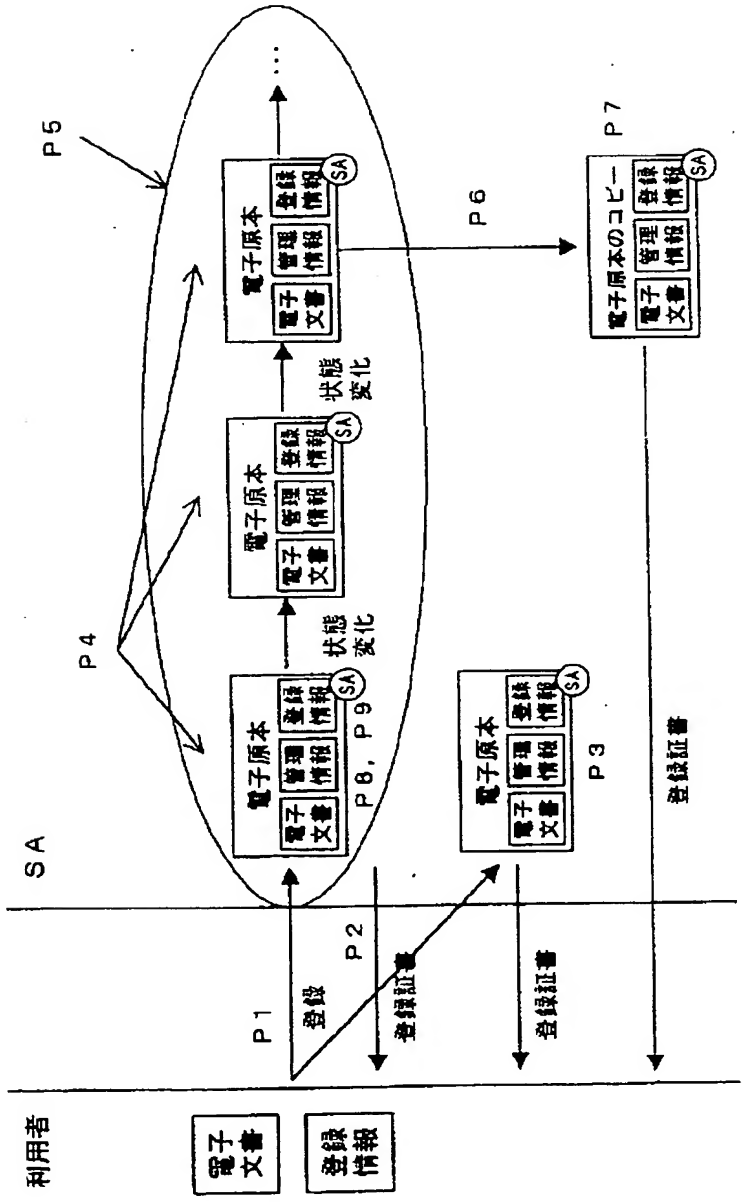
【図５】

セキュアアーカイバの処理のフローチャート



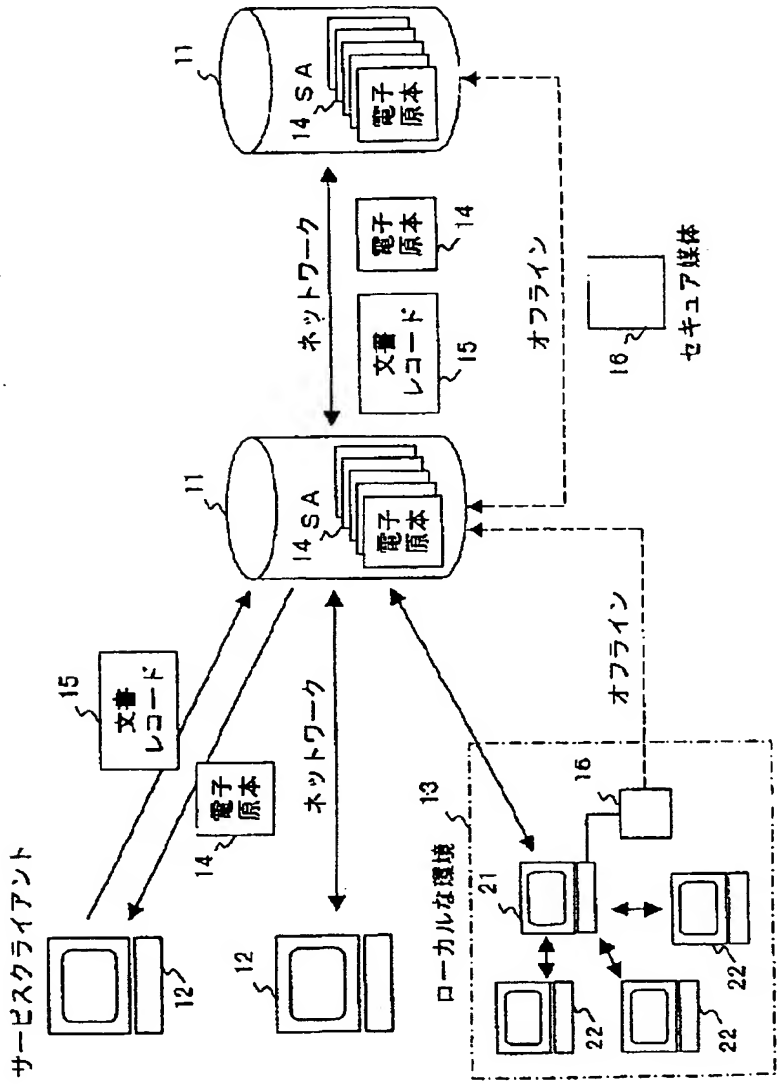
【図２】

電子原本モデルを示す図



【図３】

電子原本管理システムの構成図



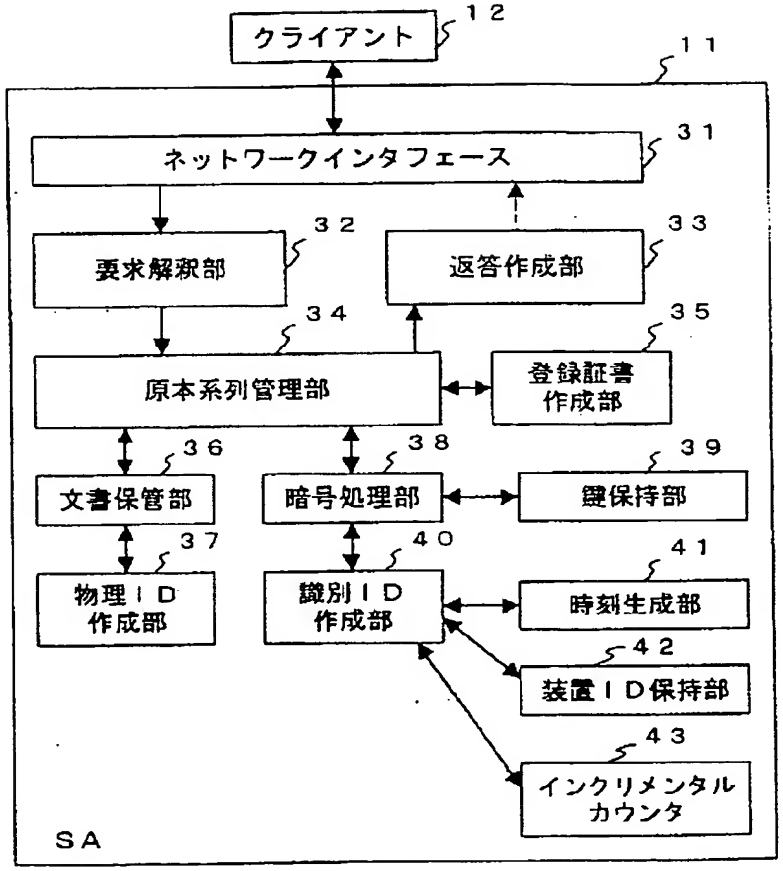
【図２６】

状態遷移情報を示す図

1998年2月17日:12:00:ユーザA:登録:SA1:ID11223344
1998年2月17日:14:00:ユーザB:原本移動:SA1:SA2
1998年2月17日:15:00:ユーザC:コピー作成
1998年2月17日:16:00:ユーザD:原本移動:SA2:SA3 (SA)

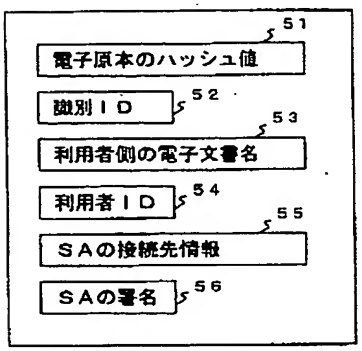
【図４】

セキュアアーカイバの構成図



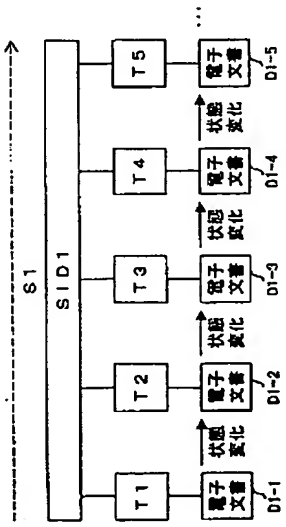
【図６】

文書レコードを示す図



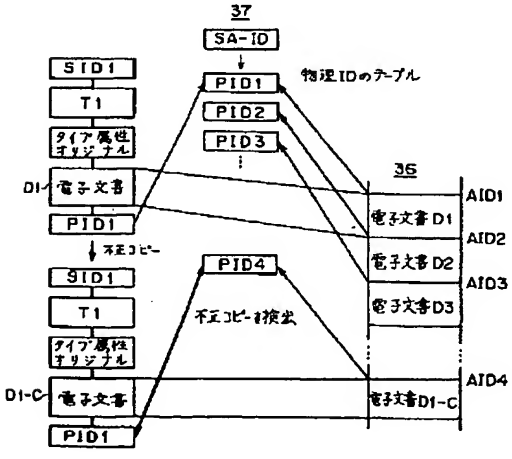
【図８】

時系列管理を示す図



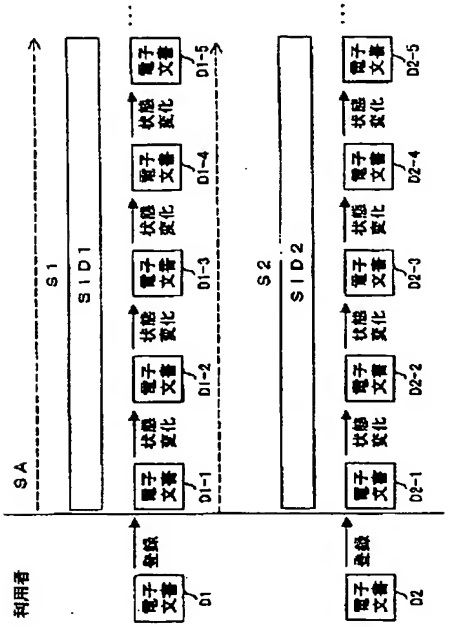
【図１２】

不正コピーの検出を示す図



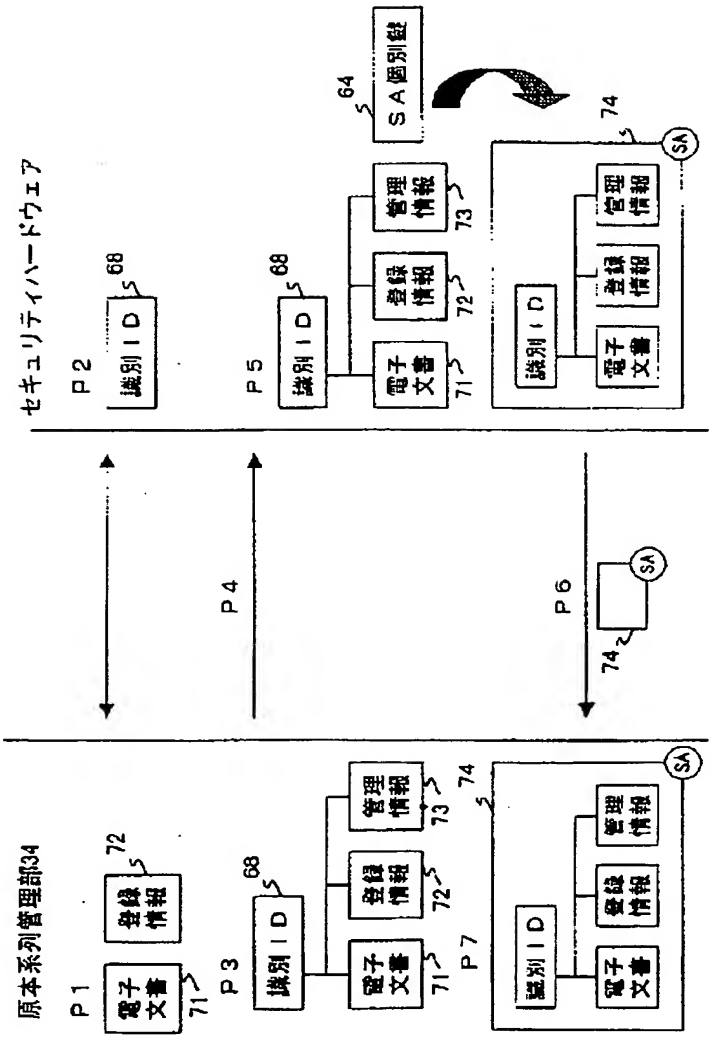
【図７】

原本系列の管理を示す図



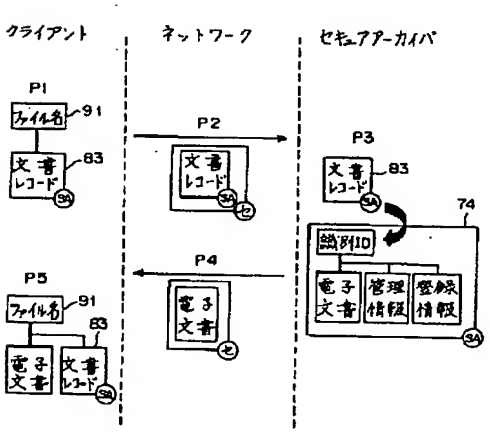
【図１５】

電子文書の保管を示す図



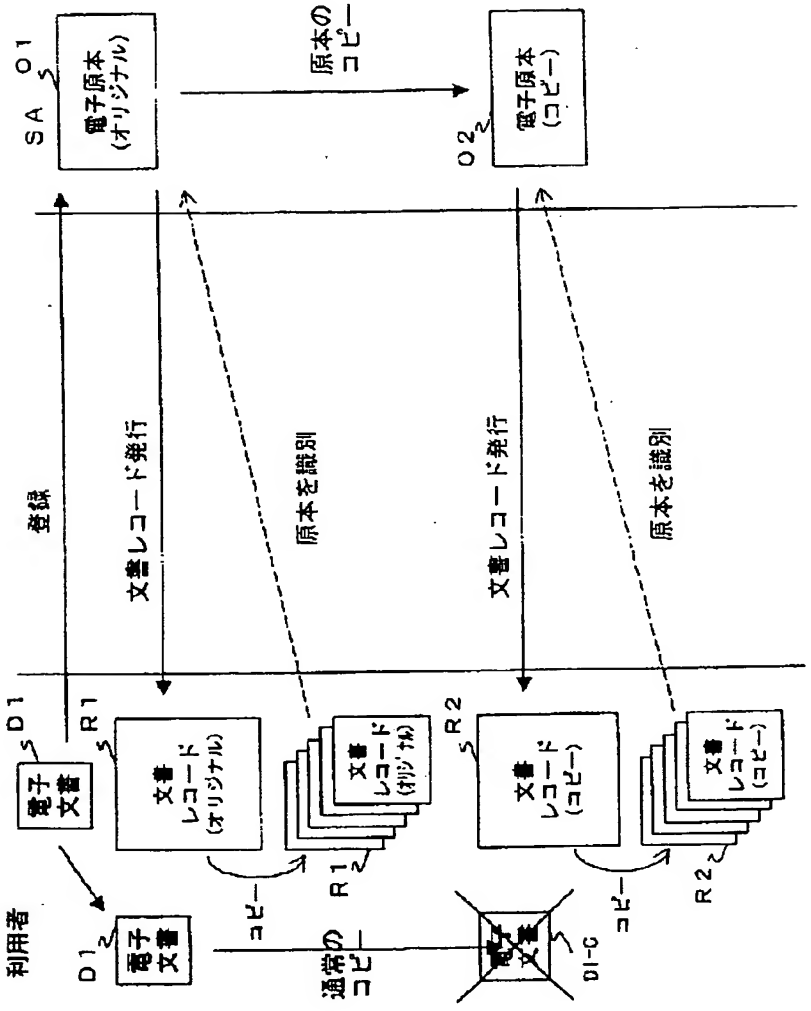
【図１８】

検索処理を示す図



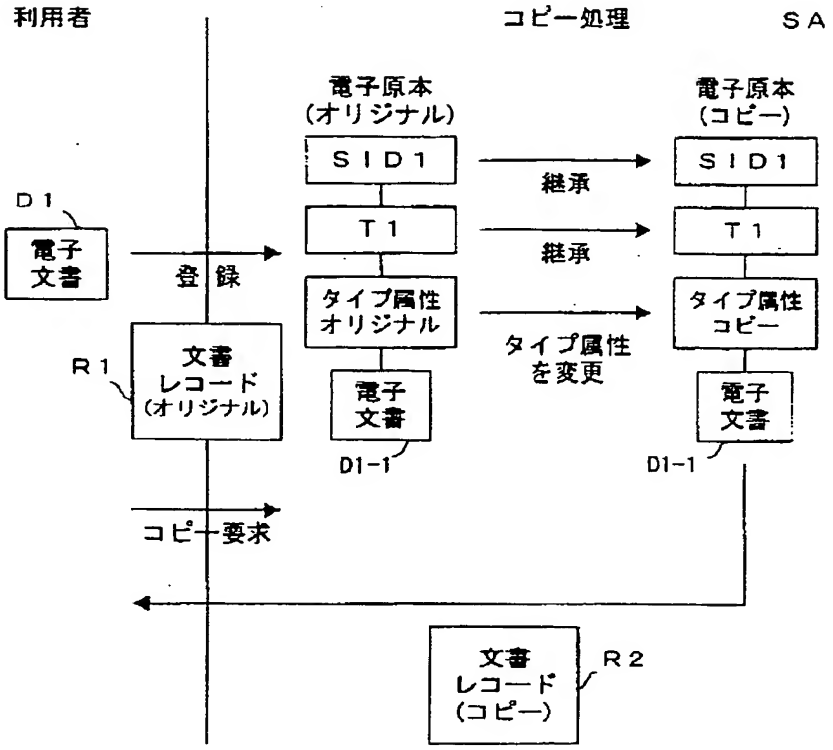
【図９】

オリジナルとコピーの識別を示す図



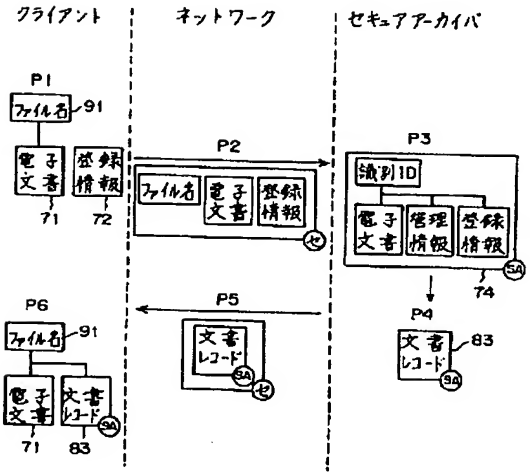
【図１０】

タイプ属性による管理を示す図



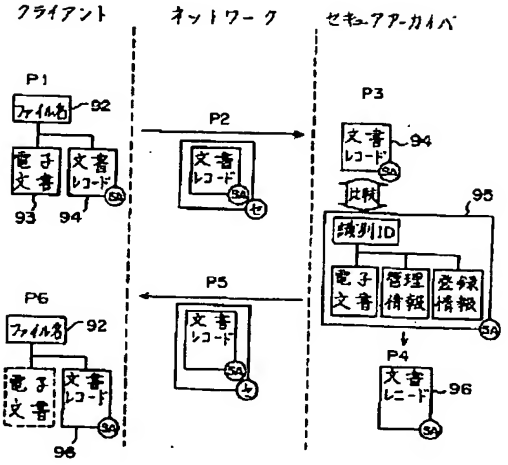
【図１７】

登録処理を示す図



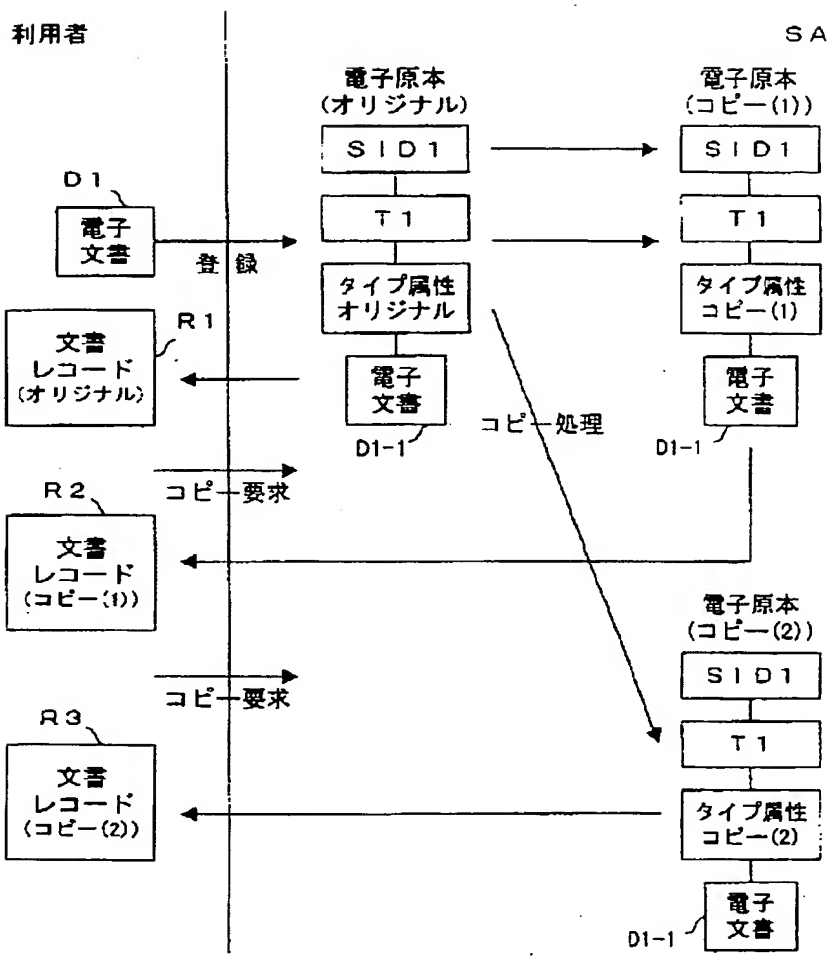
【図１９】

文書レコード検証処理を示す図



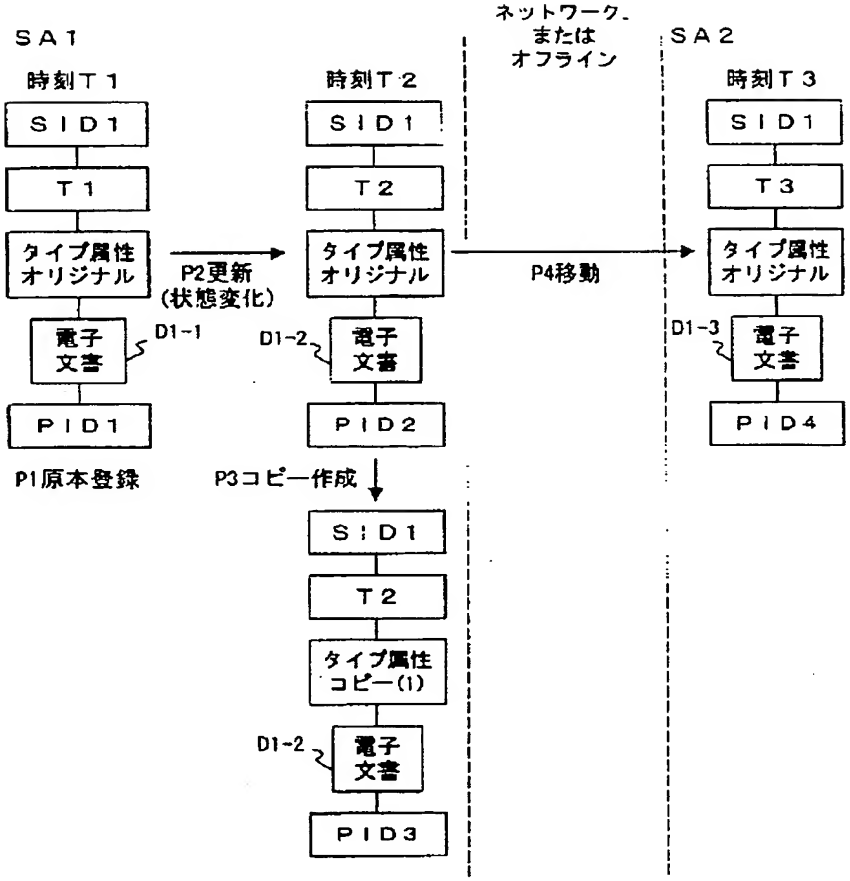
【図１１】

複数コピーの管理を示す図



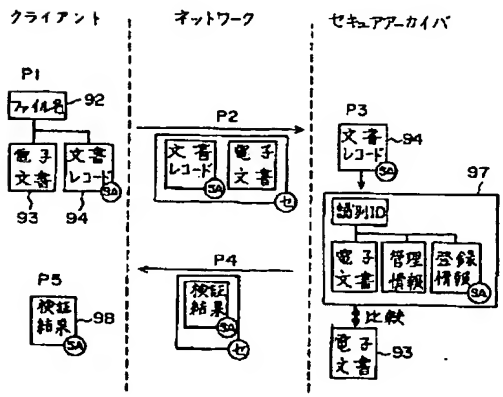
【図１３】

識　別　情　報　の　変　化　を　示　す　図



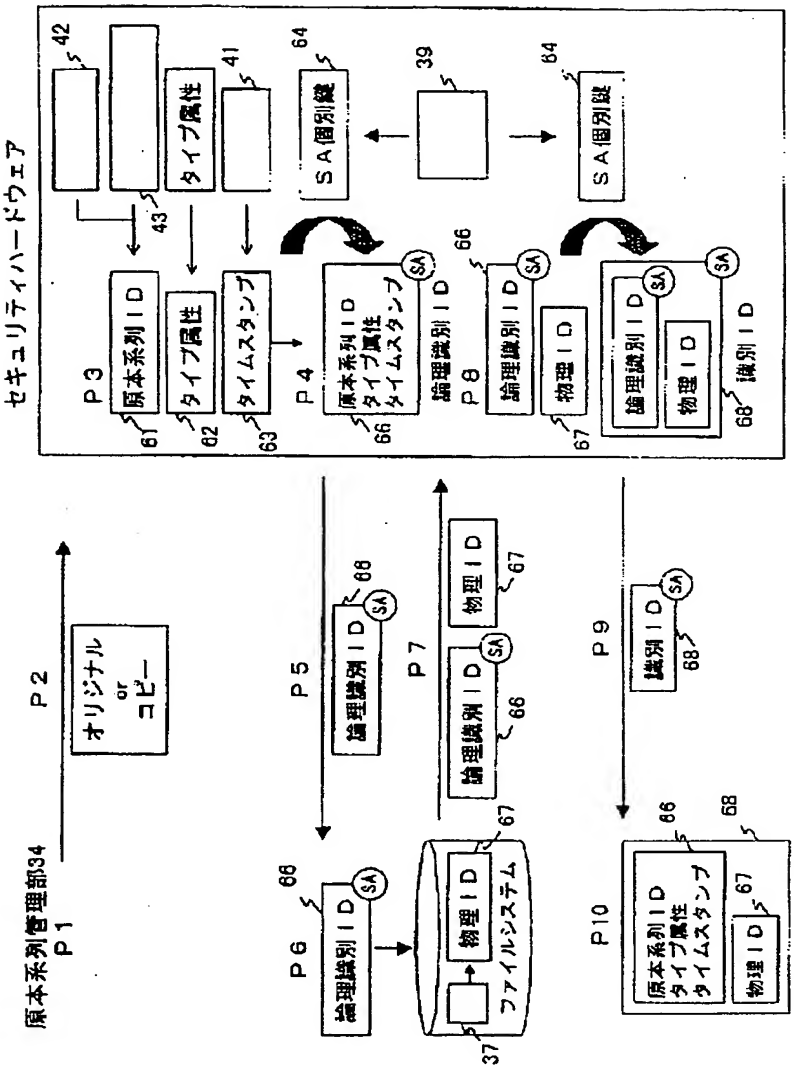
【図２０】

同一性検証処理を示す図



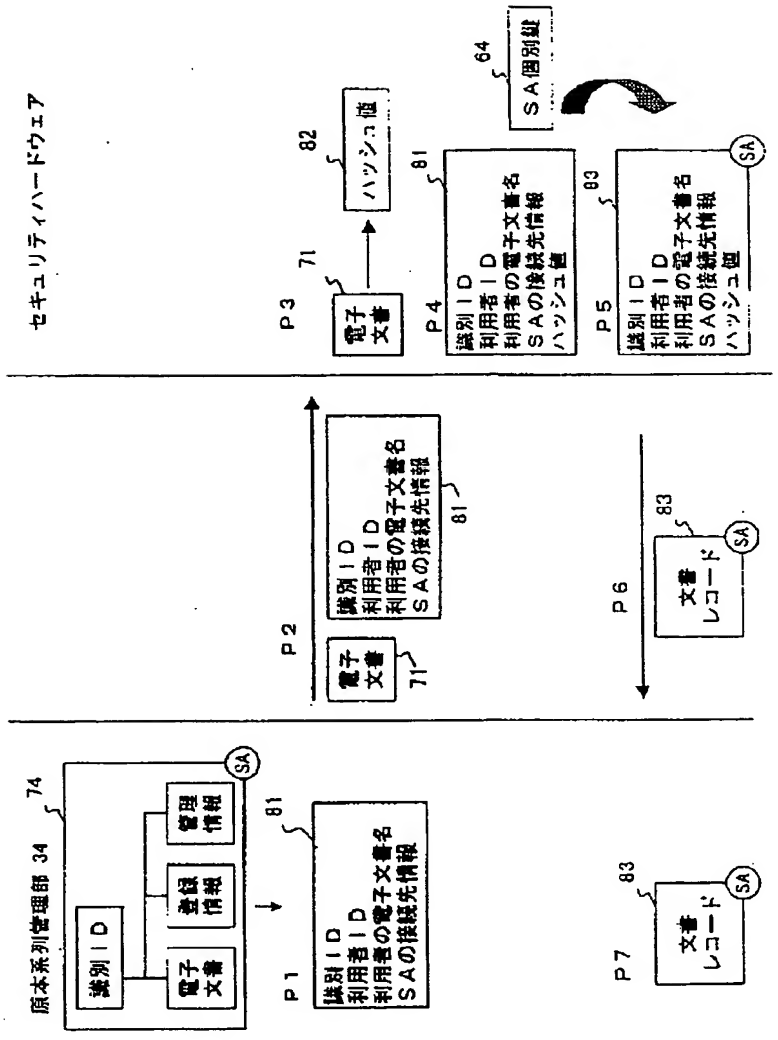
【図１４】

識別ＩＤの生成を示す図



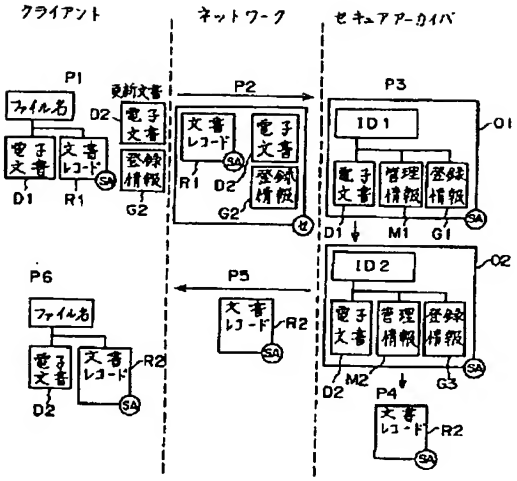
【図１６】

文書レコードの生成を示す図



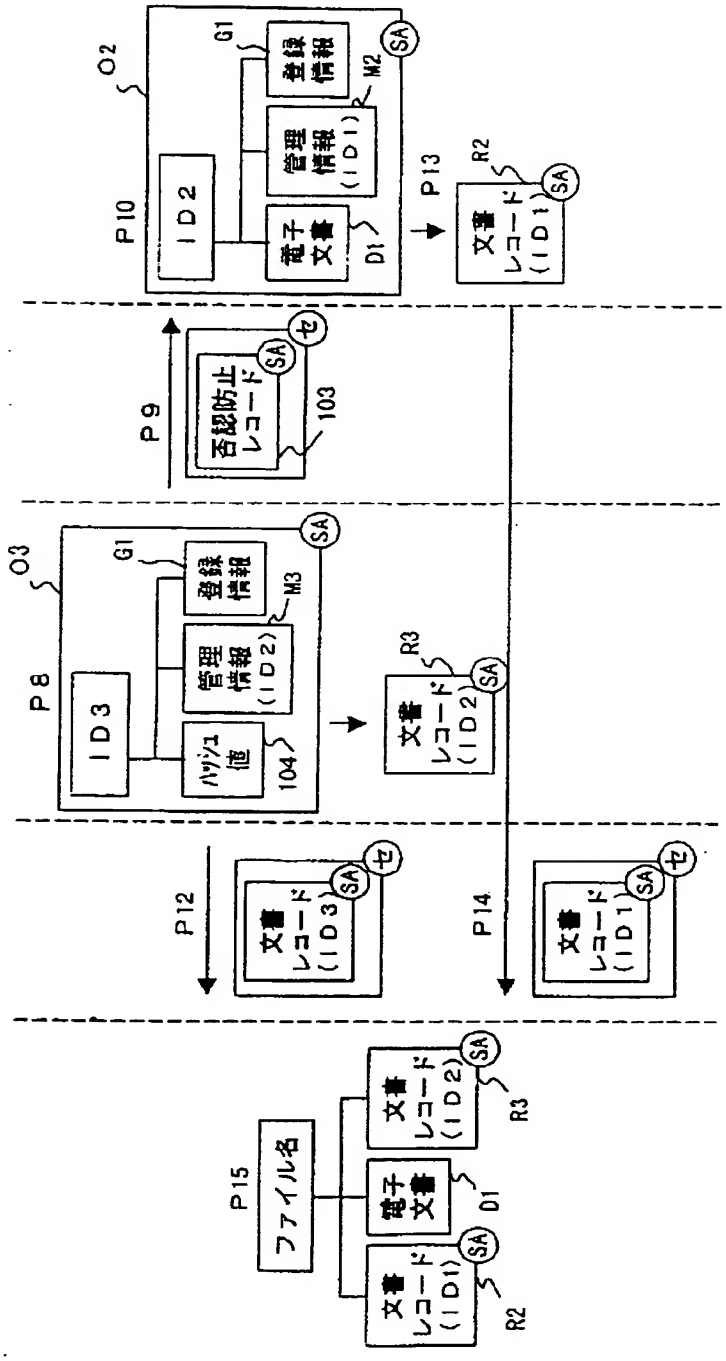
【図２１】

更新処理を示す図



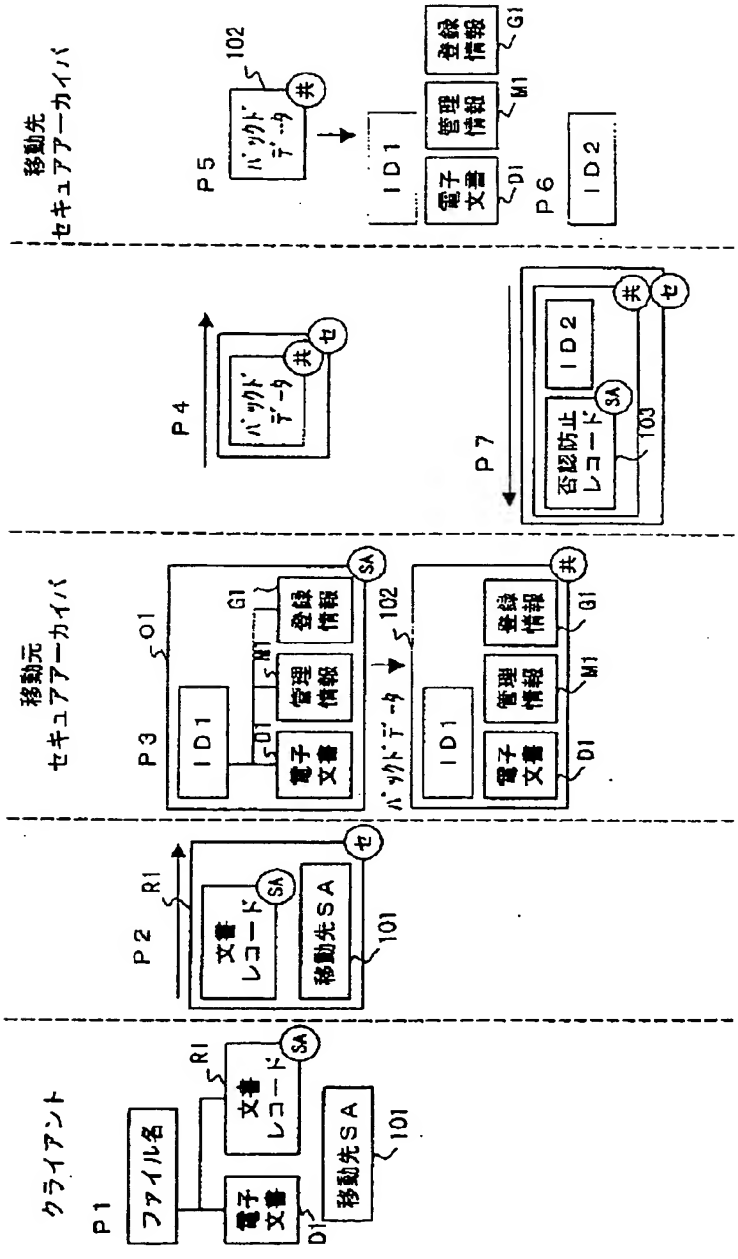
【図２３】

移動処理を示す図（その２）



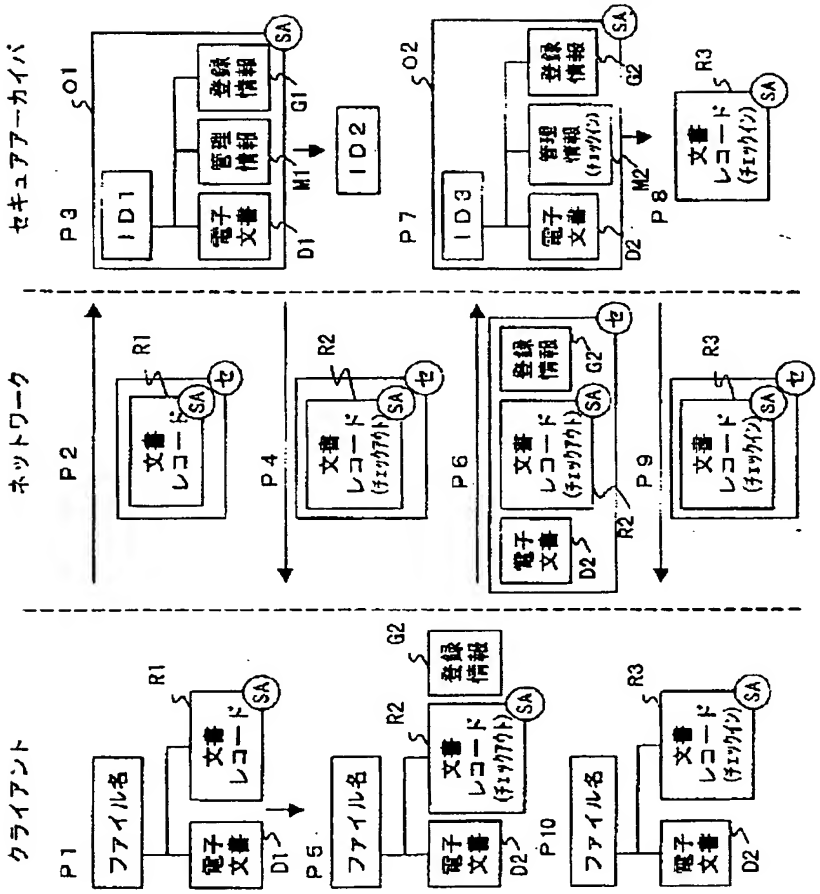
【図２２】

移動処理を示す図（その１）



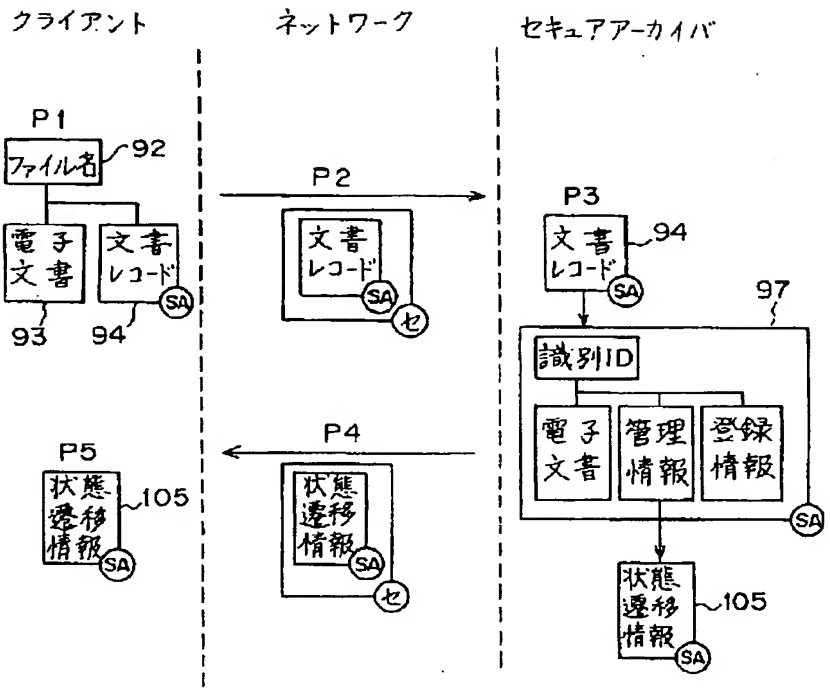
【図２４】

チェックアウト・チェックイン処理を示す図



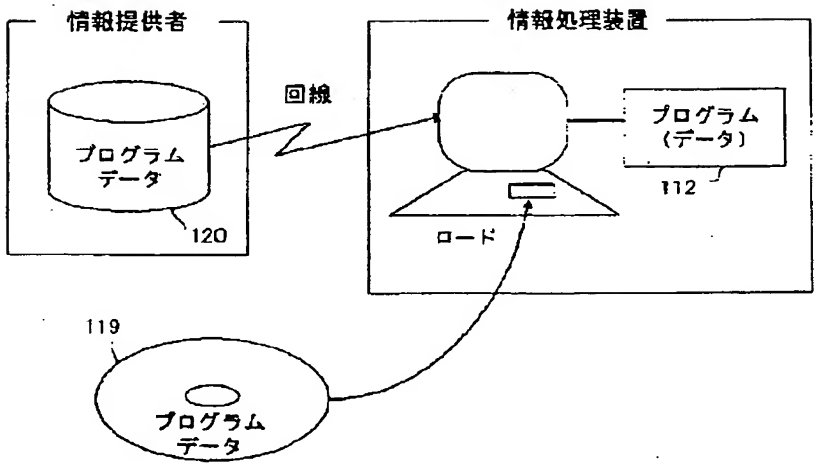
【図２５】

状態遷移取得処理を示す図



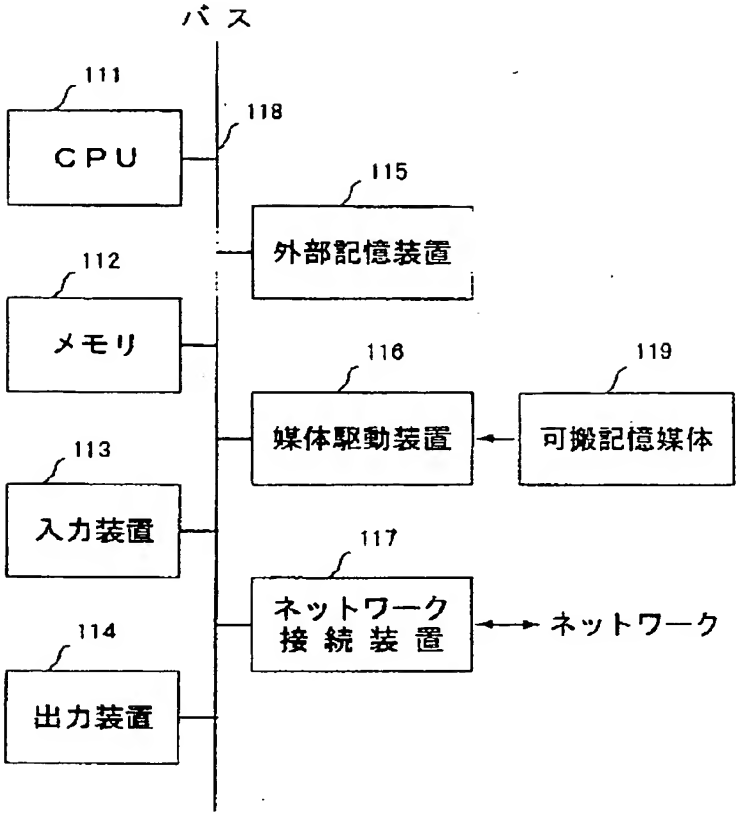
【図２８】

記　憶　媒　体　を　示　す　図



【図２７】

情　報　処　理　装　置　の　構　成　図



フロントページの続き

(72)発明者　小野　越夫
神奈川県川崎市中原区上小田中４丁目１番
１号　富士通株式会社内

Ｆターム(参考)　5B017 AA06 AA08 BA05 BA07 BB03
BB10 CA06 CA08 CA09 CA14
CA16